@gora Consommateurs : rapport de l'atelier : "commerce électronique vers la confiance"

ROYEN, Joseph; Poullet, Yves

Publication date:
1998

Document Version
le PDF de l'éditeur

@GORA98

AGORA « CONSOMMATEURS ».

Rapport de l'Atelier : « Commerce électronique : vers la confiance!!! »

Rapport présenté par :

M. Poullet Yves, Professeur à FUNDP-Namur, Directeur du CRID et responsable de l'atelier;
M. Royen Joseph, Conseiller-adjoint au Ministère des Affaires économiques à l'Administration de la Politique Commerciale, secrétaire de l'Atelier.

Bruxelles, le 16 décembre 1998.

TABLE DES MATIERES

Bruxelles, le 16 décembre 1998.

REMERCIEMENTS

Les membres de l'atelier tiennent à remercier Monsieur le Vice-Premier Ministre Elio Di Rupo, Ministre de l'Economie, des Télécommunications et du Commerce extérieur, pour son initiative et d'avoir ainsi lancé un vaste et grand débat public sur la société de l'information baptisé Agora98.

Ils tiennent tout particulièrement à le remercier de l'opportunité qui leur a été donnée de débattre publiquement de projets de lois qui ont déjà été approuvés par le Conseil des Ministres. Ils y ont vu une marque de confiance et une réelle possibilité de contribuer de manière significative à la préparation des prochains débats parlementaires. Ils se sont réjouis de pouvoir adresser au gouvernement par l'intermédiaire de Monsieur le Vice-Premier ministre des suggestions concrètes.

Ils estiment également que les assises de la société de l'information ont permis d'instaurer un véritable débat public entre les divers acteurs socio-économiques et des experts d'horizons différents sur des thèmes d'actualité et très importants pour l'avenir de notre société. Ils espèrent qu'il s'agit là de l'amorce d'un processus de dialogue constructif et continu entre les différentes parties intéressées.

Ils tiennent également à remercier le Ministère des Affaires économiques et l'Institut Belge des services Postaux et des Télécommunications pour l'aide et l'assistance continues apportées tout au long des travaux.

Enfin, ils tiennent à remercier Monsieur Lucien Van Boxstael, Directeur général de l'Administration de la Politique commerciale pour les avoir reçus si chaleureusement lors des réunions de travail et d'avoir mis en oeuvre tous les moyens nécessaires pour la réussite de ceux-ci dans une atmosphère conviviale.

INTRODUCTION GENERALE

Internet, réseaux ouverts et fermés, hyperliens, multimédia, « surfer », commerce électronique, noms de domaines, signature digitale,... : ces mots ne sont que quelques exemples de termes qui, de plus en plus, font partie de notre langage quotidien. Ce vocabulaire n'est plus réservé aux « accrocs » de l'informatique. Il préfigure le passage de notre société vers ce qu'il est convenu d'appeler la société de l'information ou l'ère digitale.

Chaque acteur de la société, que se soit en tant que citoyen, consommateur ou professionnel, est touché directement et indirectement par les différents changements.

Le commerce électronique n'est pas un phénomène nouveau. Depuis de nombreuses années, les entreprises échangent des données commerciales par le truchement de divers réseaux de communication. On assiste toutefois aujourd'hui à une expansion accélérée et à une évolution radicale, sous l'impulsion de la croissance exponentielle de l'Internet. Le commerce électronique, qui était jusqu'il y a peu à peine plus qu'une activité d'entreprise à entreprise sur des réseaux fermés exclusifs, s'étend rapidement pour constituer un tissu complexe d'activités commerciales à l'échelle planétaire entre un nombre de plus en plus important de participants, sociétés et individus, connus et inconnus, sur des réseaux ouverts comme l'Internet.

Des enquêtes et études diverses ont été effectuées sur le commerce électronique, les chiffres mettent nettement en évidence que le développement du commerce électronique interentreprises est plus rapide que celui touchant les consommateurs. Ceux-ci émettent des craintes et une certaine réticence à prendre part au commerce électronique. La concrétisation des développements potentiels est freinée par les incertitudes inhérentes aux réseaux ouverts. Les avantages du commerce électronique ne peuvent être pleinement exploités. La Commission européenne a, elle aussi, clairement mis en exergue le fait qu'il y avait lieu d'oeuvrer à renforcer la confiance des consommateurs dans le commerce électronique.[1]

Du 7 au 9 octobre 1998 à Ottawa (Canada) s'est tenu une conférence ministérielle regroupant les pays membres de l'OCDE intitulée : « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial ». La structure de cette conférence était divisée en 4 thèmes, et le premier de ces thèmes était intitulé : « Renforcer la confiance des utilisateurs et des consommateurs ». Voici une preuve de plus, s'il est encore nécessaire d'en apporter une, pour démontrer qu'il est impératif d'instaurer et de renforcer la confiance pour inciter les citoyens à recourir sans réserve aux technologies des réseaux mondiaux.

[1] Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions: « Une initiative européenne dans le domaine du commerce électronique », COM(97)157, 1997.
Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions : « Assurer la sécurité et la confiance dans la communication électronique : vers un cadre européen pour les signatures numériques et le chiffrement », COM(97)503 final, 1997.

Bruxelles, le 16 décembre 1998.

Comme signalé précédemment, la société actuelle est en marche vers une nouvelle ère. Un changement de société se traduit généralement par la perte de repères pour les citoyens qui se sentent un peu « perdus » dans le nouvel environnement qui se crée. La peur de l'inconnu est un réflexe quasi inné chez l'être humain.

L'atelier se voulait de contribuer efficacement et positivement à cette évolution et à cette mutation. Il a, dès lors, décidé d'examiner certains moyens qui pourraient permettre d'augmenter la confiance dans ce nouvel environnement. Ces thèmes étaient nombreux il semblait opportun, toutefois, de se consacrer et de se limiter à deux thèmes spécifiques afin d'apporter une contribution significative. Les thèmes retenus sont : la signature électronique et la labellisation des sites internet.

Les membres de l'atelier, persuadés de l'énorme potentiel que recèlent les nouvelles technologies de l'information ont estimé nécessaire que ce rapport tente de s'adresser à tout un chacun.

Lors de la rédaction de ce rapport, les auteurs ont tenté de refléter le consensus qui se dégageait des échanges de vues. Il est donc rédigé sous la seule responsabilité des auteurs. Les travaux au sein de l'atelier se sont voulus continus et interactifs. Chacun pouvait communiquer une note de réflexion, des remarques et des suggestions aux autres membres du groupe. Ce système d'échange permanent d'information à été particulièrement apprécié par les membres. Certains membres de l'atelier tiennent à faire part à un large public du fruit de leur propre réflexion ou de leur avis particulier sur certains points. Le lecteur soucieux d'approfondir sa réflexion, trouvera en annexe certains de ces commentaires.

Ce rapport poursuit principalement deux objectifs..

Tout d'abord, il veut répondre de façon constructive à l'invitation lancée par Monsieur le Vice-Premier Ministre Di Rupo et, en conséquence, faire part de recommandations concrètes et précises au Gouvernement quant aux thèmes examinés au sein de l'atelier.

Ensuite, il veut s'adresser également aux non-initiés afin de les aider à mieux comprendre la société de l'information qui se met en place. Toutefois, il faut rester modeste dans ses prétentions et ce rapport se limitera à donner des explications uniquement quant aux thèmes abordés dans celui-ci. Pour la partie consacrée à la signature digitale, la partie descriptive présente les projets de textes légaux en les expliquant, notamment, à la lumière des projets d'exposés des motifs. Ceci permettra au lecteur de prendre connaissance du sujet et des enjeux sans avoir à lire l'intégralité de ces projets. En ce qui concerne la labellisation des sites, l'optique retenue dans la partie descriptive consiste à présenter de manière exhaustive une expérience étrangère.

PARTIE I : LA SIGNATURE ELECTRONIQUE

I. Introduction.

Apposer sa signature sur un document, voici un acte qui s'est presque banalisé dans notre société. Chacun d'entre nous signe presque quotidiennement divers documents. La signature est un élément essentiel dans une transaction commerciale, elle marque l'accord des parties sur le contrat et identifie les parties en présence.

Nous vivons actuellement dans une société encore nettement fondée sur la prééminence de la culture de l'écrit. D'un point de vue juridique, celui qui veut prouver un acte juridique, en matière civile, dont la somme dépasse 15.000 BEF est tenu par les principes de l'article 1341 du Code civil, lequel exige que la preuve soit apportée par un écrit signé. Le législateur n'a pas donné de définition ni de l'écrit ni de la signature.

Mais, force est de devoir constater que la jurisprudence et une partie de la doctrine envisagent l'écrit comme un écrit sur un support papier et définissent la signature comme le signe par lequel une personne se présente habituellement à l'égard des tiers, accompagné d'un certain graphisme, qui est apposé de manière manuscrite sur un support papier.[2]

Toutefois, de nos jours grâce aux innovations technologiques et au développement de l'Internet les contrats peuvent se nouer dans un nouvel environnement. Une multitude d'actes juridiques sont posés quotidiennement à travers le monde sur le réseau ouvert qu'est Internet. Il est en effet d'ores et déjà possible d'acheter des produits et services par le truchement de claviers informatiques, que se soit l'achat de livre, de C.D. ou la réservation de voyages. Ces contrats, ces achats sur les autoroutes de l'information sont appelés à se développer.

Toutefois, force est de reconnaître que le système juridique existant et l'interprétation des textes légaux par la jurisprudence constituent un obstacle important au passage vers la société de l'information. Les utilisateurs des nouveaux moyens d'information et de communication ne disposent pas d'une sécurité juridique suffisante. L'incertitude quant à la possibilité de faire valoir devant le juge un contrat conclu par un nouveau moyen d'information ou la crainte que l'information transmise ne perde son caractère confidentiel sont autant de facteurs qui risquent de rendre les nouvelles technologies d'information et de communication inutiles.

Pour permettre à la société de l'information de prendre son véritable envol, il est impératif et urgent de supprimer ces entraves et de, dès lors, modifier les dispositions du Code civil relatives à la preuve des obligations. Ces modifications ne devront pas

[2] M. Antoine et D. Gobert, « Pistes et réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », in R.G.D.C., 1998, 4/5, p. 284 e.s.

nécessairement être profondes mais se devront d'actualiser les dispositions à la réalité contemporaine.

Avant d'entrer dans le coeur du sujet, il semble opportun d'apporter quelques précisions d'ordre terminologique.

Tout au long de ce rapport, nous parlerons de signature électronique et de signature digitale. Pour la bonne compréhension du lecteur il est important de préciser d'emblée que ces deux termes ne sont pas des synonymes.

Le terme signature électronique est un terme générique qui ne se réfère pas à un mécanisme de signature unique mais qui regroupe différentes technologies (code secret, techniques basées sur la cryptographie symétrique ou asymétrique, signature biométrique,....) qui méritent cette appellation dans la mesure où elles permettent la réalisation par voie électronique des fonctions de la signature manuscrite, à savoir, l'identification du signataire et l'expression de sa volonté d'adhérer au message signé.

L'ensemble des citoyens belges ont recours de manière récurrente à l'usage d'une signature électronique, sans peut-être en avoir conscience. Chacun d'entre nous dispose d'une carte de débit associée à son compte à vue (carte Bancontact/Mistercash ou carte Télépost). Lorsque le consommateur introduit sa carte dans un appareil de lecture ad hoc, il tape le montant du paiement et compose sur le clavier son code secret. Ce code secret constitue une signature électronique. Celle-ci remplace la signature manuscrite, le consommateur en composant son numéro secret indique qu'il marque son accord quant au paiement de la transaction.

La signature digitale ne constitue qu'un mécanisme particulier de signature électronique. Cette technique est considérée, à l'heure actuelle, comme celle étant la plus mûre et présentant le plus haut degré de sécurité pour les échanges de données en réseau ouvert. Elle est basée sur la technique de cryptographie asymétrique.

La cryptographie est une branche des mathématiques appliquées qui consiste à transformer des messages en des formes apparemment inintelligibles pour les restituer ensuite dans leur forme initiale.

Après ces quelques précisions utiles, nous vous invitons à lire le rapport relatif aux travaux de l'atelier sur la signature électronique. Tout d'abord quelques explications et un exemple concret devraient permettre de mieux comprendre le fonctionnement de la signature digitale. Ensuite, les documents ayant servi de base aux travaux seront présentés. Par après, le lecteur pourra prendre connaissance d'un résumé des travaux et réflexions de l'atelier, avant finalement de découvrir les recommandations finales émises par les participants aux travaux.

II. Explication du fonctionnement de la signature digitale.

Pour faciliter la lecture et la compréhension de ce rapport, il semble utile, voire nécessaire de présenter et de tenter d'expliquer le fonctionnement de la signature digitale.

L'utilisation d'une signature digitale constitue tout un processus, on peut y distinguer 10 étapes[3] :

1. l'utilisateur crée ou se voit attribuer une paire de clés cryptographique qui lui est propre;
2. l'expéditeur rédige un message sur l'ordinateur;
3. l'expéditeur prépare un abrégé de son message, à l'aide d'un calcul algorithmique sûr. La création de la signature digitale utilise le résultat contrôle d'un calcul qui est à la fois dérivé du message signé et d'une clé privée donnée et qui est unique. Pour assurer la sûreté du résultat du calcul, il est impératif qu'il n'y ait qu'une possibilité infime que la même signature digitale puisse être créée par la combinaison de tout autre message ou de tout autre clé;
4. l'expéditeur chiffre l'abrégé du message à l'aide de la clé privée. Celle-ci s'applique à l'abrégé du message à l'aide d'un algorithme mathématique. La signature digitale est constituée par l'abrégé du message ainsi chiffré;
5. l'expéditeur, le plus souvent, attache ou ajoute sa signature digitale au message;
6. l'expéditeur envoie sa signature digitale et son message (chiffré ou non) au destinataire par voie électronique;
7. Le destinataire utilise la clé publique de l'émetteur pour vérifier la signature de l'expéditeur. La vérification à l'aide de la clé publique de l'expéditeur prouve que le message provient exclusivement de cet expéditeur là;
8. le destinataire créée lui aussi un « abrégé du message » à l'aide du même algorithme;
9. le destinataire compare les deux abrégés de message. S'ils sont identiques, alors le destinataire sait que le message n'a pas été modifié après avoir été signé. Même si le message a subi une très légère modification après avoir reçu une signature digitale, l'abrégé du message créé par le destinataire sera différent de celui créé par l'expéditeur;
10. Le destinataire se voit délivrer un certificat par un tiers authentificateur qui confirme le lien entre la clé publique et l'expéditeur du message. Le certificat comprend également d'autres renseignements qui peuvent être certifiés par cette autorité de certification.

Voici, à présent, un exemple concret qui montre les mécanismes du fonctionnement de la signature digitale.

Alice désire envoyer à Baert un message informatisé signé de façon électronique. Après avoir réalisé un condensé de ce message au moyen d'une opération ma-

[3] travaux de la CNUDCI, Groupe de travail sur le commerce électronique, 31ième session, http://www.un.or.at/uncitral

thématique. Ce condensé est le résultat d'une fonction appelée fonction de hachage irréversible. Cette fonction permet de générer de façon concise une chaîne de données qui représente le message en question. Cette représentation est sécuritaire, très précise et permet de détecter tout changement apporté au message. En effet, il suffit au destinataire d'appliquer la fonction de hachage au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été altéré en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature digitale (ou numérique). Alice envoie alors à Baert son message (en clair) accompagné de la signature digitale.

Lorsque Baert reçoit le message et la signature digitale, il décode cette dernière en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Baert est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice; il sait alors de manière certaine qu'elle est l'auteur du message pour autant qu'une tierce partie (une autorité de certification) certifie que cette clé publique est bien celle d'Alice. Grâce à la fonction d'hachage, l'intégrité du message d'Alice peut être garantie.

Il n'est pas inutile de signaler que la réalisation d'un condensé du message à l'aide de la fonction de hachage irréversible n'est pas indispensable. En effet, l'émetteur du message pourrait directement encoder le message avec sa clé privée sans nécessairement passer par la production du condensé. Néanmoins, la fonction de hachage irréversible sera souvent utilisée dans un souci de gagner du temps : encoder avec la clé privée un condensé (fichier de petite taille) est plus rapide que l'encodage du message en clair (fichier du plus grosse taille).[4]

La lecture de ces explications et illustration pourrait laisser croire que l'utilisation d'une signature digitale est compliquée et réservée à des experts en informatique ou mathématique. Certes, il est vrai que cette procédure repose sur un processus compliqué, mais dans la pratique un logiciel convivial cache la complexité du système et facilite l'utilisation de cette nouvelle forme de signature afin de la rendre accessible à tout un chacun.

Cet exemple met également en lumière le rôle important qu'une tierce partie est appelée à jouer, il s'agit de l'autorité de certification. Tout au long de ce rapport nous utiliserons l'abréviation usuelle A.C., lorsque nous ferons référence à une autorité de certification.

[4] Mireille Antoine et Didier Gobert, op.cit. , p.285 et s.

III. Les documents de base aux travaux.

Pour lancer ses travaux et la réflexion, l'atelier s'est essentiellement basé sur trois projets de textes légaux : deux avant-projets de loi fédérale et une proposition de directive européenne. Nous proposons au lecteur de faire connaissance, à présent, avec ces textes grâce à la brève présentation qui en est donnée. Cette présentation doit lui permettre de mieux comprendre l'intégralité du rapport. Le lecteur trouvera, en annexe de ce présent rapport, ces projets.

1. Deux avant-projets de lois.

Le 12 juin 1998, le Conseil des Ministres a approuvé deux avant projets de lois importants pour favoriser le développement de la société de l'information. Le premier avant-projet concerne l'activité d'autorité de certification agréée, le second vise à modifier certaines dispositions du Code Civil relatives à la preuve des obligations.

Voici le texte des communiqués de presse officiel relatif à ces deux projets publiés à l'issue de ce Conseil des Ministres.

1. *« Le Conseil des Ministres a approuvé un avant-projet de loi relatif à l'activité d'autorité de certification agréée. Cette approbation porte sur l'utilisation de signatures digitales.*

La signature digitale est un mécanisme parmi d'autres de signature électronique. Elle constitue cependant le mécanisme le plus mûr technologiquement. C'est aussi le mécanisme le plus sûr pour les échanges dans un réseau ouvert comme celui d'Internet.

Une réglementation juridique en cette matière est essentielle pour le développement du commerce électronique. Ce type de commerce offre, pour les prochaines années, d'énormes possibilités économiques.

Le principe de la signature digitale est basé sur un système de double clés, appelé "cryptographie asymétrique". La personne qui désire disposer d'une signature digitale reçoit d'une autorité de certification, deux clés (qui sont en fait des programmes électroniques) : une clé privée et une clé publique. L'autorité de certification ne donnera cette paire de clés qu'après avoir vérifié l'identité du demandeur auprès d'une administration locale.

La clé privée permet à la fois de certifier l'identité de l'expéditeur du message et de crypter son message. La clé publique, permet quant, à elle de décrypter le message. Cette clé publique doit être connue du destinataire. Toutes les clés publiques seront donc répertoriées sur Internet afin d'être consultables par tout le monde . Des dispositions pour la protection de la vie privée et pour la protection des consommateurs ont également été prises. »

2. « Le Conseil des Ministres a approuvé un avant-projet de loi visant à modifier certaines dispositions du Code Civil relatives à la preuve des obligations.

Cet avant-projet a pour but d'adapter les règles de la preuve du Code Civil aux besoins de la société de l'information et plus précisément à l'échange et à l'archivage de données par voie électronique.

L'avant-projet de loi confirme en premier lieu un principe général figurant déjà dans le droit belge, à savoir qu'une partie à une convention doit être protégée contre des clauses qui entraînent une répartition inégale de la charge de la preuve. Cette mesure a pour but de protéger en particulier les consommateurs. Les nouvelles mesures visent à éviter en effet qu'ils supportent seuls le risque de l'utilisation des nouvelles technologies et les problèmes de preuve qui peuvent en découler.

En deuxième lieu, il est expressément disposé qu'outre la signature manuscrite classique, "l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit" peut également être considérée comme une signature.

Enfin, un document portant une signature électronique pourra désormais être considéré comme un acte sous seing privé original, pourvu qu'il soit établi avec certitude que l'intégrité du contenu du document est bien conservée ».

Pour des questions de facilités, lorsque dans le rapport, il sera question du projet de loi relatif à l'activité d'autorités de certification en vue de l'utilisation de signatures digitales, nous utiliserons l'appellation : « projet de loi A.C. ». Lorsqu'il sera fait référence au projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations, nous convenons d'utiliser l'abréviation « projet de loi Code civil ».

1.1. Brève présentation du projet de loi Code civil.

Le gouvernement, conscient que l'absence d'un cadre juridique pour l'emploi de signatures électroniques constitue un frein important au développement de la société de l'information et une menace pour les consommateurs a adopté le 30 mai 1997 une note préconisant la création d'un tel cadre juridique.[5]

Différentes solutions s'offrent au législateur pour admettre la signature électronique:[6]

a) instauration d'un régime de liberté probatoire.

Cette solution consisterait à modifier la loi afin qu'elle n'exige plus qu'un acte juridique supérieur à 15.000 BEF soit prouvé par un écrit signé. Cette solution aurait pour effet de rendre tout mode de preuve recevable, en ce compris la preuve électronique, en cas de litige. Cette solution est insatisfaisante car elle bouleverserait totalement

[5] Pour un extrait de cette note, voyez J. Dumortier et P. Van Eecke, « Naar een juridische regeling van de digitale handtekening in Belgie », Computerrecht, 1997/4, 154-159.
[6] M. Antoine et D. Gobert, op.cit.,p.285 et s.

notre système juridique, et d'autre part elle laisserait l'appréciation des modes de preuve au pouvoir discrétionnaire du juge, ce qui ne solutionnerait pas le problème.

b) élévation du seuil en deçà duquel la preuve est libre.

Cette alternative constituerait à augmenter la limite de 15.000 BEF fixée à l'article 1341 du Code civil. Ceci augmenterait le nombre d'actes juridiques pour lesquels la preuve peut être apportée librement. Cette alternative ne résout pas le problème, car elle maintient la suprématie de l'écrit papier signé manuscritement et n'apporte aucun élément de réponse quant à la valeur probante qu'il convient d'apporter aux documents signés électroniquement.

c) légitimation de la preuve électronique par le biais d'exception.

Cette solution consisterait à étendre le champ d'application de l'article 1347 (commencement de preuve par écrit) ou 1348 (impossibilité de se procurer une preuve écrite). Ceci n'est pas suffisant car le commencement d'une preuve par écrit suppose un écrit et d'autre part l'impossibilité de se procurer une preuve écrit doit être involontaire. De plus, une réforme de ce type pourrait vider l'article 1341 de son contenu en instaurant un régime de liberté probatoire (cfr.a)

d) approche ouverte et fonctionnelle des concepts du Code civil.

La doctrine est unanime pour reconnaître à la signature une double fonctions : identification du signataire et manifestation de volonté de ce dernier de s'approprier le contenu de l'acte auquel la signature se réfère. Par ailleurs la signature manuscrite combinée à l'écrit papier permet d'assurer l'intégrité du contenu.

C'est cette approche qui a été retenue dans le projet de loi qui a été approuvé par le Conseil des Ministres.

Le but principal de ce projet de loi est d'adapter les règles de la preuve du Code civil aux besoins de la société moderne de l'information et plus précisément à l'échange et à l'archivage des données par voie électronique, sans cependant réformer fondamentalement les principes essentiels de notre droit de la preuve.

L'article 2 vise à compléter l'article 1315 du Code civil. L'article 1315 actuel dispose que celui qui exige l'exécution d'une obligation doit en prouver l'existence. Inversement, celui qui prétend être libéré, doit fournir la preuve du paiement ou du fait qui a causé l'extinction de son obligation.

En pratique, cette liberté contractuelle a souvent comme conséquence qu'une partie économiquement plus faible, par manque de connaissance juridique, souscrit à un régime de preuve très désavantageux, qui fait reposer la charge de la preuve en ce qui concerne les transactions électroniques en grande partie sur ces épaules. Afin de protéger cette partie, un troisième alinéa est ajouté à l'article 1315 CC, afin de préciser que les conventions qui dérogent au régime de preuve de cet article, sont réputées

nulles à moins qu'elles ne soient conclues après le commencement d'un procès judiciaire.

L'article 3 vise à compléter l'article 1322 CC de la façon suivante :

« *Est assimilé à la signature manuscrite l'ensemble des données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit.*
En cas d'application de l'alinéa précédent, est assimilé à un acte sous seing privé original l'écrit signé dont le maintien de l'intégrité du contenu est établi avec certitude».

Cette définition constitue en quelque sorte une révolution en Belgique car elle s'oppose à la définition de la signature formelle adoptée par la jurisprudence belge et consacrée par la Cour de Cassation.

Ce libellé ne vise pas uniquement la signature digitale, la définition est large et ouverte et en conséquence couvre d'autres types de signatures électroniques. Cette définition ouverte et fonctionnelle rend inutile de définir la notion d'écrit. La jurisprudence et la doctrine s'accordent de plus en plus pour considérer qu'il convient d'interpréter largement cette notion et qu'il ne faut pas considérer comme écrit le seul texte manuscrit ou imprimé sur un support papier.

Le juge devra, dans le cas d'espèce qui lui est soumis, vérifier si la signature électronique utilisée permet d'établir avec **certitude** l'identité de l'auteur et son adhésion au contenu de l'écrit. Pour ce faire, le juge dispose de différents critères d'appréciation dont[7] :

- le degré de perfectionnement du matériel utilisé par chacune des parties;
- la nature de leur activité commerciale;
- la fréquence avec laquelle elles effectuent entre elles des opérations commerciales;
- la nature et l'ampleur de l'opération;
- le statut et la fonction de la signature dans un régime législatif et réglementaire donné;
- la capacité des systèmes de communication;
- la série de procédures d'authentification communiquée par un intermédiaire;
- l'observation des coutumes et des pratiques commerciales;
- l'existence de mécanismes d'assurance contre les messages non autorisés;
- l'importance et la valeur de l'information contenue dans le message de données;
- la disponibilité d'autres méthodes d'identification et le coût de leur mise en oeuvre;
- le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données à été communiqué;

[7] Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique, 1996, p.38 et 39, http://www.un.or.at/uncitral, cité par M. antoine et D. Gobert, op.cit, p. 291.

1.2. Projet de loi A.C. agréée.

L'exemple et les premières explications relatifs au fonctionnement d'une signature digitale ont mis en évidence que l'utilisation d'une telle signature nécessitait l'intervention d'une tierce partie à la transaction qui unit l'émetteur d'un message et son destinataire, cette partie supplémentaire c'est l'autorité de certification. Pour renforcer la sécurité et la confiance dans l'utilisation de la signature digitale et dans les A.C., il est nécessaire d'établir un cadre juridique qui détermine les droits et obligations des A.C.. Toutefois une A.C. n'est pas obligée de se soumettre aux règles énoncées dans ce texte légal, elle n'y sera soumise que si elle souhaite obtenir une agréation. Dès lors, sur le marché il va coexister des A.C. agréées et non agréées. Toutes les deux pourront exercer leurs activités, toutefois, l'optique retenue par le gouvernement belge est d'accorder la valeur d'une signature à l'utilisation de clès certifiées par une A.C. agréée, voire de rendre obligatoire le passage par une A.C. agréée en particulier dans le cadre de certaines relations entre administrations et administrés.

Ce projet de loi comprend trois chapitres. Le premier contient des définitions et détermine l'objectif et le champ d'application de la loi. Le second fixe les conditions d'agréation. Le troisième établit le régime juridique applicable aux autorités de certifications agrées.

L'article second définit certains termes utilisés dans le projet de lois : signature digitale, certificat, autorité de certification, titulaire de certificat, administration, entité.

Il semble indiqué d'attirer l'attention toute particulière du lecteur sur la définition du « titulaire de certificat ». En effet, tant une personne physique que morale peut se voire délivrer un certificat, il en est de même pour une association de fait.[8]

L'article 3 précise le champ d'application de la loi. Le second paragraphe de cet article consacre le principe de la libre agréation, selon lequel une A.C. est libre de demander ou pas une agréation. Une autorité de certification n'a donc pas l'obligation de demander une agréation pour exercer des activités de création, de délivrance et de gestion des certificats. Il pourra ainsi coexister sur le marché des A.C. agréées et non agréées. Le troisième paragraphe consacre le principe de la variabilité du contenu variable des agréations. Une A.C. pourrait se spécialiser dans la certification d'un tel ou tel attribut (ex.: profession). En vertu du paragraphe 4 de ce même article 3, nul ne peut être contraint de recourir à une A.C. Toutefois, ce principe est tempéré par le second alinéa qui prévoit que pour certaines relations ou transactions qui exigent un niveau de sécurité et de fiabilité une norme légale pourrait imposer que si une personne recourt à une signature digitale celle-ci doit être combinée à un certificat émis par une A.C. agréée.

[8] Nous renvoyons le lecteur au point IV.6 relatif à la signature des personnes morales.

Le paragraphe 5 de cet article 3 est très important car il crée un lien entre le présent projet et le projet Code civil. On peut en effet considérer que d'une part la signature digitale présente un degré de sécurité suffisant et que le dispositif sécuritaire qui entoure les AC agréées confère à la signature digitale un niveau de sécurité et de fiabilité au moins équivalent à la signature manuscrite. De ce fait, la signature digitale pourra produire les mêmes effets juridiques qu'une signature manuscrite.

L'article 4 fixe les conditions qui doivent impérativement être remplies par une A.C. pour obtenir une agréation. Celles-ci seront précisées par un arrêté royal délibéré en Conseil des Ministres.

Les articles 5 à 9 précisent les missions d'une autorité de certification. Une A.C. ne peut ni enregistrer, ni conserver, ni reconstituer la clé privée. Elle crée et délivre un ou plusieurs certificats à tout candidat titulaire qui en fait la demande. Elle procure au candidat titulaire les informations nécessaires à l'utilisation correcte et sûre de ces services.

Il est important de souligner, pour éviter toute confusion, que les autorités de certification ne certifient pas une signature. La principale fonction d'une autorité de certification est d'assurer un lien formel entre une personne et sa clef publique. Ce lien sera confirmé dans un certificat digital émis par l'autorité de certification.

L'autorité de certification conserve un registre électronique accessible en permanence à toute personne par voie électronique. Ce registre comprend les certificats délivrés par l'A.C. et, le cas échéant, le moment de leur suspension et de leur révocation. Ce registre doit être protégé contre toute modification non autorisée.

L'article 10 traite du contenu du certificat. Dans un certificat on peut trouver deux types d'informations. D'une part, il y a les informations minimales obligatoires imposées par la loi. D'autre part, le certificat peut contenir d'autres informations. Dans cette hypothèse, l'A.C. est tenue d'indiquer dans le certificat si elle certifie ou non ces informations supplémentaires (ex. : profession, n° de compte bancaire,...).

L'article 11 prévoit les obligations du titulaire de certificat. Celui-ci est seul responsable de la confidentialité et de l'intégrité de sa clé privée.

Les articles 12 à 14 abordent les problématiques de suspension et de révocation de certificat.

La suspension vise à interrompre jusqu'à nouvel ordre l'usage d'un certificat. Cela implique d'une part que le titulaire ne puisse utiliser le certificat et, d'autre part, que le destinataire ne puisse se fier au certificat suspendu. Elle peut avoir lieu à la demande du titulaire ou d'office par l'A.C.. Lorsque le titulaire fait la demande, l'A.C. doit s'exécuter, que la demande soit ou non motivée. La suspension à l'initiative de l'A.C. ne peut avoir lieu que s'il existe des raisons sérieuses et motivées pour admettre que le certificat a, par exemple, été délivré sur base d'informations erronées ou falsifiées.

La révocation, quant à elle, vise à mettre fin au certificat avant son terme. Cette décision est irréversible. Elle peut avoir lieu à la demande du titulaire ou à l'initiative de l'A.C.. Tout comme pour la suspension, si le titulaire demande la révocation, l'A.C. doit s'exécuter, que la demande soit motivée ou non, après avoir vérifié et établi que cette demande provient bien du titulaire. Si la révocation est le fait de l'A.C., elle doit être motivée et le titulaire doit être immédiatement informé.

L'article 15 prévoit des dispositions en cas d'arrêt volontaire ou involontaire de l'activité d'une A.C.

L'article 16 prévoit des mesures pour garantir la protection de la vie privée. L'A.C. ne peut collecter que des données à caractère personnel que si elles sont nécessaires à l'exercice des ses missions et elles ne peuvent être utilisées que dans le cadre des activités de certification.

Afin de revêtir une réelle utilité, toute infrastructure de certification adoptée à un niveau international doit être envisagée dans une perspective internationale. L'article 17 de ce projet de loi, en traitant de la reconnaissance transfrontière des certificats, fait écho à cette préoccupation. Les certificats étrangers pourront être assimilés à des certificats émis par des A.C. belges agréées s'ils présentent un niveau de sécurité équivalent à celui qui est exigé par cette loi.

L'article 18 traite l'aspect de la fiabilité technique. La fiabilité et l'adéquation du niveau de sécurité sont appréciées en fonction de l'état de technique tel qu'arrêté et rendu public par l'Administration ou toute entité désignée par elle. Cette procédure a été délibérément choisie pour rester souple par rapport aux évolutions technologiques

Les articles 19 et 20 traitent de la responsabilités. L'article 19 traite de la responsabilité des A.C. et prévoit qu'il appartiendra au Roi de fixer les montants minimal et maximal en-deçà et au-delà desquels les parties ne peuvent limiter ou étendre la responsabilité de l'A.C.. L'article 20, quant à lui, traite de la responsabilité du titulaire (ex. : communication d'informations erronées).

L'article 21 donne mission à l'administration de contrôler les A.C. agréées, en vérifiant qu'elle se conforme à la loi et à ses arrêtés d'application. Le contrôle peut aboutir au retrait de l'agréation.

L'article 22 prévoit des sanctions civiles et pénales notamment en cas d'usurpation du titre d'A.C. agréée.

2. Une proposition de directive européenne.

Constatant que les initiatives législatives en matière de signature électronique se multipliaient au sein des Etats membres de l'Union Européenne, la Commission a estimé qu'il était nécessaire et urgent d'avoir un cadre juridique harmonisé au niveau européen afin d'éviter que le fonctionnement du marché intérieur ne soit gravement entravé.

Le 13 mai 1998 elle a présenté une proposition de directive du Parlement Européen et du Conseil sur un cadre commun pour les signatures électroniques[9].

Cette proposition est le fruit d'une réflexion amorcée à la suite de la Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions: « Une initiative européenne dans le domaine du commerce électronique »[10]. Par après la Commission a présenté une Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions : « Assurer la sécurité et la confiance dans la communication électronique : vers un cadre européen pour les signatures numériques et le chiffrement »[11]. Le 1er décembre 1997, le Conseil a accueilli favorablement cette communication et a invité la Commission à soumettre dès que possible une proposition de directive au Parlement européen et au Conseil sur les signatures numériques.

Les principaux aspects de la directive proposée sont les suivants[12] :

exigences essentielles: cette proposition définira des exigences essentielles pour les certificats attestant la signature numérique et les services de certification, afin de garantir un niveau minimal de sécurité et de permettre la libre circulation de ces certificats et de ces services dans l'ensemble du marché unique. Ces exigences porteront notamment sur la fiabilité des prestataires et sur l'utilisation de systèmes dignes de confiance;

responsabilité: cette proposition fixera des règles minimales en matière de responsabilité des prestataires de services qui seront responsables notamment de la validité du contenu du certificat. Cette approche garantira la libre circulation des certificats et des services de certification dan le marché unique, permettra de gagner la confiance des consommateurs, et encouragera les opérateurs à concevoir des systèmes et des signatures sûrs, sans prévoir une réglementation restrictive et rigide;

reconnaissance juridique: cette proposition stipulera qu'aucune discrimination juridique ne pourra s'exercer à l'encontre d'une signature électronique pour la seule raison qu'elle se présente sous une forme électronique, car il est essentiel pour la mise en place d'un système ouvert et fiable de signatures électroniques que ces signatures aient des effets juridiques. Si un certificat et le prestataire de services répondent à certaines exigences essentielles, on considérera automatiquement que les signatures électroniques qui s'appuient sur ses services jouissent de la même reconnaissance légale que les signatures manuscrites. En outre, elles pourront être acceptées comme preuve dans une procédure judiciaire;

cadre neutre du point de vue technologique: étant donné le rythme de l'innovation technologique, cette proposition prévoit la reconnaissance juridique des signatures

[9] COM(1998) 297 final. http://www.ispo.cec.be/eif/policy/Welcome.html#digital
[10] COM(97)157, 1997. http://www.cordis.lu/esprit/src/ecomcom.htm
[11] COM(97)503 final, 1997. http://www.ispo.cec.be/eif/policy/Welcome.html#digital
[12] Voir le communiqué de presse de la Commisison : http://europa.eu.int/comm/dg15/

électroniques, indépendamment de la technologie utilisée (par exemple les signatures numériques reposant sur la cryptographie asymétrique ou la biométrie);

champ d'application: cette proposition concerne la fourniture au public de certificats visant à identifier l'expéditeur d'un message électronique, mais elle ne s'applique pas aux groupes fermés d'utilisateurs tels que les intranets ou les systèmes bancaires, dans lesquels une relation de confiance existe déjà, et où, par conséquent, il n'existe pas de besoin manifeste de réglementation;

certification: des services de certification pourront en principe être offerts sans autorisation préalable, étant donné l'évolution rapide de la technologie et du marché, et du fait que les forces du marché encourageront le développement d'un niveau élevé de sécurité pour répondre aux préoccupations des consommateurs. Les Etats membres seront libres d'instituer des régimes volontaires d'accréditation pour les prestataires de services de certification, afin d'indiquer des mesures ou des niveaux de sécurité particuliers. Les prestataires de services de certification désireux de voir les utilisateurs de leurs certificats bénéficier d'une reconnaissance légale des signatures s'appuyant sur leurs certificats devront cependant remplir certaines conditions essentielles;

dimension internationale: afin de faciliter le commerce électronique au niveau mondial, cette proposition prévoit des mécanismes de coopération avec les pays tiers en matière de reconnaissance mutuelle des certificats, sur la base d'accords bilatéraux et multilatéraux.

IV. LES TRAVAUX DE L'ATELIER.

1. Précisions terminologiques.

Lors des travaux il est apparu, à plusieurs reprises, qu'il pouvait exister des problèmes de compréhension entre les membres en raison des termes utilisés. Il semble donc opportun d'apporter certaines précisions d'ordre terminologique.

Tout d'abord nous renvoyons le lecteur à l'introduction pour ce qui concerne la distinction entre signature digitale et signature électronique.

Il y a lieu également d'attirer l'attention sur les différences qui existent entre les fonctions d'enregistrement et de certification. L'enregistrement, préalable à la certification, consiste à collecter de manière fiable et sécurisée les informations destinées à figurer sur le certificat (nom, prénom, profession, n° registre de commerce,....) et à émettre des documents attestant la véracité de ces informations (ex. : certificat d'inscription à l'ordre des avocats ou à l'ordre des médecins). Cette fonction d'enregistrement peut être réalisée par l'AC. Elle peut également être confiée à une autorité d'enregistrement distincte de l'A.C (ex. : commune, ordre professionnel, chambre de commerce,...).

Donc il y a deux fonctions, opérations ou rôles distincts qui peuvent être exécutés par une même société ou par deux différentes :

1° Préciser que telle personne physique est bien celle-là et , le cas échéant, que les attributs ou renseignements destinés à figurer sur le certificat lui correspondent[13];

2° Assurer un lien formel entre une personne et sa clé publique. L'autorité de certification doit également s'assurer de la possession par la demandeur du certificat, de la clé privée associée à la clé publique.

Cette distinction est importante, notamment, lorsque l'on s'interroge sur les questions des responsabilités. Dans leur contrat avec les autorités d'enregistrement, les autorités de certification, seules responsables vis à vis des tiers, veilleront à reporter la responsabilité vers les autorités d'enregistrement en cas d'erreurs dans les informations transmises par ces dernières.

Dans ce rapport il est, à de multiples reprises, fait référence aux termes « signature digitale » et « agréation des A.C. ». Un membre a tenu à faire remarquer qu'il y aurait lieu de remplacer le mot « digitale » par « numérique » en français. L'adjectif « digital », en français, signifie qui appartient aux doigts. Dès lors l'anglicisme « digital » semble déconseillé. Le mot « agréation » est considéré comme un belgicisme. Il serait préférable d'utiliser le terme « agrément ».

Bien que ces précisions semblent fondées, le rapport utilisera les termes « digitale » et « agréation » pour ne pas provoquer de confusion, étant donné qu'ils sont utilisés dans les projets de loi.

2. La neutralité technologique.

Les technologies et les mécanismes utilisés pour l'authentification et la certification continuent à se développer à l'échelle mondiale. En raison de la rapidité du progrès technologique en la matière, il est important que le cadre normatif qui veut être mis en place ne constitue pas un frein à l'innovation et permettent l'amélioration des technologies déjà utilisées et n'empêchent pas l'apparition de nouveaux mécanismes d'authentification.

Cette neutralité technologique doit également permettre le développement de nouveaux mécanismes dans un climat de saine concurrence.

[13] Cette première fonction pourrait être scindée en deux sous-fonctions. Tout d'abord celle du nomage, par laquelle une qualité est reconnue à une personne, ensuite celle de l'enregistrement, par laquelle les différentes qualités et l'identité de la personne se trouvent répertoriées.

2.1. Permettre l'émergence de nouvelles technologies.

La majorité des membres de l'atelier marquent leur satisfaction quant à la proposition de modification de l'article 1322 du Code civil :

> « *Est assimilé à une signature manuscrite l'ensemble des données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit.*
> *En cas d'application de l'alinéa précédent, est assimilé à un acte sous seing privé original, l'écrit signé dont le maintien de l'intégrité du contenu est établi avec certitude* ».

La définition donnée au premier alinéa est large et ne se limite pas à viser le signature digitale. Elle se veut non discriminatoire à l'égard des technologies. L'équivalence fonctionnelle peut être rencontrée par différentes techniques qu'il s'agisse de la reconnaissance de caractéristiques biométriques, de la cryptographie symétrique ou asymétrique. Il appartiendra au juge de vérifier, dans le cas d'espèce qui lui est soumis si les exigences fonctionnelles de la signature sont présentes, à savoir : l'identité de l'auteur de l'écrit et son adhésion au contenu.

Certains membres, toutefois, suggèrent de modifier les termes « est établi avec certitude ». Ils estiment qu'aucun technologie ne peut être considérée comme fiable à 100%, et qu'en conséquence il serait plus raisonnable et adéquat de faire référence à une présomption raisonnable. Aussi, ils proposent de libeller l'article de la façon suivante :

> *« Est assimilé à la signature manuscrite, l'ensemble des données issues de la transformation de l'écriture et qui peut être attribué à une personne déterminée .*
> *En application de l'alinéa précédent, l'écriture signée dont le maintien de l'intégrité du contenu est établi avec certitude, est assimilée à un acte sous seing privé original ».*

Enfin, les membres marquent leur satisfaction quant à l'option retenue visant à ne pas définir le terme « écrit ». Ceci permet une interprétation large. L'absence de définition légale permet de ne pas freiner les développements technologiques.

2.2. Permettre l'évolution de la signature digitale.

Il est important que dans le projet de loi relatif aux A.C. agréés, les dispositions n'empêchent pas le développement de cette technologie.

L'article 18 du projet de loi répond à ce souci. Plutôt que de définir sur base de critères techniques, qui deviendraient très vite obsolètes, le caractère fiable des moyens techniques ainsi que le caractère adéquat du niveau de sécurité, l'article 18 définit le caractère fiable et adéquat sur base de risques que l'on désire éviter et des dangers que l'on veut écarter. Les caractères fiable et adéquat des moyens techniques et du niveau de sécurité seront satisfaits dès lors que ceux-ci permettent notamment

d'éviter ou de détecter toute atteinte à l'intégrité d'un message signé digitalement ou d'un certificat et toute utilisation non autorisée d'une clé privée.

En vue de rester souple par rapport aux évolutions technologiques, la fiabilité des moyens techniques ainsi que l'adéquation du niveau de sécurité sont appréciées en fonction de l'état de la technique au moment où cette appréciation est faite. Afin de donner aux A.C. des indications quant à cet état de la technique celui-ci est arrêté régulièrement par l'administration ou toute entité désignée par elle et est rendu public.[14] A cet égard, on se référera à des standards adoptés internationalement.

3. Le jeu de la concurrence.

La mise à disposition d'un certificat est un service, lequel se trouve sur un marché qui doit être concurrentiel. La concurrence doit jouer entre les différentes A.C. agréées ou non. Pour ce qui est des A.C. agréés, si l'on veut que la concurrence soit maximale et donc bénéfique, différents principes doivent être respectés à différents niveaux.

Il apparaît important de fixer des conditions certes minimales mais qui soient suffisantes afin d'obtenir un niveau de sécurité adéquat. En effet, il serait délicat, du point de vue de la concurrence, d'adopter des conditions à ce point contraignantes qu'aucune ou qu'une seule A.C. ne puisse être agréée. De plus, en fixant un niveau minimal de sécurité, on laisse aux A.C. agréées la possibilité d'offrir un niveau de sécurité supérieur et de la sorte, la possibilité de se faire concurrence par ce biais que ce soit quant aux tarifs pratiqués ou à la qualité du service rendu.

On est en droit de se demander si les accords actuels et futurs conclus entre une A.C. déterminée et une autorité d'enregistrement précise ne sont pas de nature à restreindre ou fausser la concurrence. En effet, si une A.C. conclut un accord d'exclusivité avec, par exemple, l'ordre national des avocats ou des médecins, celle-ci ne risque-t-elle pas d'obtenir le monopole de la certification des avocats ou des médecins?

Enfin, le Conseil des Ministres a adopté le 11 septembre 1998 un arrêté royal qui introduit un système provisoire de signature électronique pour la sécurité sociale. L'article premier de cet arrêté royal fait référence à une A.C. qui serait agréée par la Banque-Carrefour, sans toutefois déterminer les conditions d'agréation. La Banque-Carrefour pourrait donc décider arbitrairement, étant donnée l'absence de critères, d'agréer ou de refuser l'agréation à l'une ou l'autre A.C., voire de se satisfaire d'une seule A.C. agréée. Ceci semble totalement inacceptable sur le plan du droit de la concurrence.[15]

[14] Avant-projet de loi relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales, exposé des motifs, p. 30 et 31.

[15] Pour de plus amples informations, sur cet arrêté royal, il y a lieu de se référer au point IV.12

4. Le contenu d'un certificat.

L'article 10 du projet de loi A.C. agréée, traite du contenu du certificat. Deux types d'informations peuvent être présentes dans un certificat : les informations obligatoires et les informations facultatives.

4.1. Les informations obligatoires (article 10 §1).

On dénombre 6 informations différentes qui doivent impérativement figurer dans tous les certificats.

> *« 1. les nom et prénom, tout autre renseignement pertinent permettant d'identifier le titulaire du certificat ou, le cas échéant, le pseudonyme de la personne physique qui en fait la demande, précédé de l'indication qu'il s'agit d'un pseudonyme;*
>
> *2. La clé publique du titulaire;*
>
> *3. la référence aux algorithmes nécessaires pour utiliser la clé publique du titulaire du certificat ainsi que la clé publique de l'autorité de certification;*[16]
>
> *4. le code d'identification du certificat;*
>
> *5. la date d'émission et la date d'expiration du certificat;*
>
> *6. les données d'identification et d'agréation de l'autorité de certification ».*

Il appartient à l'A.C. de prendre toutes les mesures nécessaires afin d'établir l'exactitude des informations contenues dans le certificat. Nous reviendrons également ultérieurement sur la façon dont les A.C. peuvent collecter et vérifier des informations au regard des exigences des règles de protection de la vie privée.[17]

A propos de l'identification des personnes physiques, il convient de souligner que la loi réserve au titulaire du certificat la possibilité de conserver l'anonymat par l'utilisation d'un pseudonyme. Cette disposition fait écho de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des personnes.

Il est à noter que le commentaire de l'article 10 (page 18 de l'exposé des motifs) exprime de manière claire que : « le texte prévoit toutefois que le Roi, sur la proposition des Ministres des Affaires économiques, de la Santé publique, des Affaires sociales et de l'Emploi et du travail, peut fixer des cas limitatifs dans lesquels l'usage d'un pseudonyme ne sera pas admis. Cette restriction vise notamment à éviter toute fraude ou abus dans les relations avec les organismes de la sécurité sociale.». Or, on ce doit de constater que l'article 10 ne dit rien à ce propos.

[16] L'opportunité d'inclure la clé publique de l'autorité de certification dans le certificat est contestée.
[17] Voir infra, protection de la vie privée, point IV.9 du rapport.

4.2. Les informations accessoires (article 10, §2).

Outre les informations obligatoires qui devront figurer sur le certificat, celui-ci peut également contenir d'autres informations facultatives. Ces informations viseront à préciser un ou plusieurs attributs du titulaire du certificat (ex. : profession, ...). Les A.C. ne sont pas tenues de certifier ces informations, elles peuvent se contenter de les ajouter sur le certificat mais, dans cette hypothèse, en précisant qu'elle ne les certifient pas.

Ce système de certificat à contenu variable pourrait permettre une spécialisation de certaines A.C.. Il permettra également de stimuler la concurrence entre les A.C.. Il ne faut pas perdre de vue qu'au plus il y aura des informations certifiées sur le certificat au plus le prix de celui-ci sera élevé.

Si l'A.C. ne souhaite pas ou n'a pas les moyens de certifier ces autres informations, elle doit préciser clairement et de façon non équivoque sur le certificat qu'elles ne sont pas certifiées.

5. Les A.C. sans moyens pour remplir leurs missions?

Lors des débats de l'atelier certains membres estimaient que la loi impose une charge (certifier certaines informations) et donc, une responsabilité aux A.C. agréées sans leur donner les moyens adéquats.

Il semble nécessaire d'opérer une distinction, pour éclaircir ce débat, entre les informations relatives à l'identité du titulaire et les autres informations.

a) identité du titulaire.

L'article 10 de l'avant-projet prévoit que le certificat doit au moins contenir " les nom et prénom, tout autre renseignement, permettant d'identifier le titulaire du certificat".

L'exposé des motifs de l'avant-projet de loi nous aide à mieux comprendre la ratio legis de cette disposition :

"L'autorité de certification ne peut se baser que sur les renseignements qui lui sont fournis par le candidat titulaire. Par exception, le Roi pourra imposer des conditions plus strictes pour le contrôle de l'identité des personnes lorsque le certificat qui sera délivré peut être utilisé dans des relations avec les autorités publiques. Dans ce cas spécifique, le Roi pourra notamment exiger que l'autorité de certification vérifie l'identité de la personne par référence avec le numéro de registre national de cette dernière". (exposé des motifs de l'avant projet de loi, article 7, page 15).

L'optique privilégiée est de donner plus de moyens aux A.C. agréées lorsque le certificat est délivré en vue d'une utilisation avec les autorités publiques.[18]

b. Les autres informations.

En ce qui concerne les autres informations, celles qui ne sont pas obligatoires, il y a lieu de se référer au second paragraphe de l'article 10 du projet de l'arrêté royal :

"En outre, le certificat peut contenir d'autres informations. L'autorité de certification n'est cependant pas tenue de confirmer ces dernières. Elle indique dans le certificat le caractère confirmé ou non de chaque information".

Peut-on estimer que cette disposition est suffisante pour que les A.C puissent certifier un attribut particulier ou toutes autres informations? Le texte ne délègue aucun pouvoir au Roi pour conférer aux A.C. des moyens pour vérifier ou collecter les informations communiquées par le candidat titulaire.

Pour des raisons légitimes de protection de la vie privée, l'article 16§1 prévoit :"(...)La collecte d'informations auprès de tierces personnes peut uniquement avoir lieu avec le consentement du candidat titulaire ou du titulaire du certificat".

Dans l'esprit du projet, si les personnes physiques souhaitent voir figurer sur leur certificat d'autres informations que celles relatives à l'identité, elles devront autoriser l'A.C à vérifier ces informations auprès d'une autorité d'enregistrement (ex. : ordre professionnel,...).

Enfin, il est a souligner que le contenu minimal du certificat ne correspond pas à celui prévu par l'annexe I du projet de directive européenne. Dans le projet de texte européen, on prévoit notamment que doit figurer dans le certificat (h) les limites éventuelles à l'utilisation du certificat et (i) les limites à la responsabilité du prestataire de service de certification et la valeur des transactions pour lesquelles le certificat est valable, le cas échéant.

6. La signature électronique des personnes morales.

Permettre aux personnes morales de signer, voici une nouvelle question qui fait jour à la suite des progrès techniques. En effet, jusqu'à présent la question ne se posait pas vu que la signature était uniquement manuscrite et que dès lors une personne morale, qui n'a pas d'existence matérielle, pouvait difficilement signer manuscritement.

Le projet de loi A.C. agréées permet aux personnes morales d'obtenir un certificat mais ne leur reconnaît pas la possibilité de signer au sens du Code civil. En effet, l'article 5§3 du projet de loi dispose :

[18] Nous renvoyons le lecteur au point IV.9 consacré à la protection de la vie privée.

« Sans préjudice des articles 1323 et suivants du Code civil, une signature digitale réalisée sur base d'un certificat émis dans les conditions fixées par la présente loi constitue une signature au sens de l'article 1322 du Code civil lorsqu'elle est appliquée à cette fin par une personne physique ».[19]

Personne ne semble contester la certification des personnes morales. Ne faudrait-il pas aller plus loin? Un document dont la signature digitale serait effectuée sur base d'un certificat émis par une A.C. agréée au nom d'une personne morale serait considéré comme un acte sous seing privé et non comme un document réputé non signé qui n'a la valeur d'une simple présomption sur le plan du droit de la preuve.

L'ajout « lorsqu'elle est appliquée à cette fin par une personne physique » empêche d'aller dans ce sens et constitue même une sorte de régression, ou en tout cas un obstacle à toute évolution de la jurisprudence. En effet, le Code civil ne fait aucune référence au fait que la signature est réservée aux personnes physiques. Seules la jurisprudence et la doctrine estime que la signature est un attribut propre à la personne physique. Dès lors, les derniers mots de cet article constitue un véritable obstacle à une évolution jurisprudentielle compte tenu notamment des nouvelles technologies.

Lors des débats, les membres n'ont pas réussi à atteindre un consensus sur ce débat particulier. Il parait toutefois très intéressant de signaler les principaux arguments avancés en défaveur et en faveur de l'octroi d'une signature aux personnes morales.

6.1. en défaveur de l'octroi d'une signature aux personnes morales.

- Une telle option ne pourrait que créer un hiatus entre l'engagement dans le monde physique et électronique.

- Depuis 1804, les règles du Code civil et celles en droit des sociétés en matière de délégation sont suffisantes et n'ont pas empêché le développement des transactions commerciales.

- D'un point de vue purement juridique, outre la modification profonde du concept de la personne morale qui intervient en donnant à la personne morale le droit d'agir autrement que par ses organes, et ce uniquement dans le monde électronique, l'introduction de la signature des personnes morales implique de profonds remaniements notamment dans le droit des sociétés. A cet égard, il suffit de se référer au principe de base du droit des sociétés repris à l'article 8 des lois coordonnées sur les sociétés commerciales. La conséquence de ce qui précède est qu'il ne peut être question d'aborder cette problématique par le petit bout de la lorgnette qui est le droit de la preuve.[20]

- Accorder une signature aux personnes morales ne serait d'aucune utilité.

- Il faut pouvoir trouver un responsable, une personne physique responsable.

[19] Souligné par les auteurs du rapport.

[20] Toutefois, cet argument doit être relativisé, compte tenu du fait que la personne morale ne pourra opposer aux tiers la non habilitation d'un employé à l'engager.

- Certains actes nécessitent la signature de deux personnes déléguées au sein d'une société.

D'un point de vue commercial, la solution actuelle, par laquelle une personne morale agit au travers de ses organes, est applicable à la signature digitale. En effet, par un certificat, la personne morale reconnaît que les personnes à qui des pouvoirs ont été délégués ont bien ces pouvoirs. On peut simplement réfléchir par analogie aux délégations de pouvoir qui, dans une entreprise, sont généralement accordées par le conseil d'administration et le l'administrateur délégué.

Pour des raisons évidentes de facilités et d'efficacité, il est préférable de calquer le monde électronique sur le monde réel.

6.2. En faveur de l'octroi d'une signature aux personnes morales.

- Le développement du commerce électronique est essentiellement celui interentreprises. Le commerce électronique qui concerne les consommateurs est marginal bien qu'il soit appelé à se développer rapidement. Dès lors cette nouvelle forme de commerce touche essentiellement des personnes morales.

- Il est techniquement très facile de vérifier l'existence et l'identité d'une personne morale (exemple : acte constitutif publié au Moniteur belge). On peut même se demander s'il n'est pas plus facile de vérifier l'identité d'une personne morale que celle d'une personne physique.

- Si elle n'existe pas matériellement la personne morale existe juridiquement et à ce titre elle est apte à être titulaire de droits et d'obligations ainsi qu'elle est susceptible de voir sa responsabilité civile engagée. Les deux fonctions d'une signature sont d'une part l'identification et d'autre part, la volonté d'être engagé par l'acte signé. Il est facile d'identifier une personne morale. Signer un acte, c'est aussi exprimer la volonté d'être engagé par l'acte signé, et de ce fait créer des droits et obligations dans le chef du signataire, la signature digitale combinée à un certificat permet de réaliser cette seconde fonction.

- Il existe une tendance actuelle à reconnaître la responsabilité pénal des personnes morales . En France, l'article 121-2 du Code pénal reconnaît expressément la responsabilité pénale des personnes morales.

- Une personne morale doit pouvoir faire des milliers d'opérations automatiquement par voie électronique (déclaration de TVA, acceptation des demandes par le site web d'une entreprise commerciale). Une personne physique habilitée par la société à signer n'acceptera jamais de laisser sa clé privée dans un ordinateur pour signer les opérations. Cet argument justifie que la loi reconnaisse dès maintenant la signature de l'A.C., personne morale.

- Dans l'Union Européenne, certains pays (états nordiques, Italie, Royaume-Uni et Pays- Bas) sont favorables à une telle approche, dès lors aller dans un autre sens poserait des problèmes au niveau de la reconnaissance mutuelle des certificats. Cela

pourrait également inciter les personnes morales belges à aller « se faire certifier » dans les pays voisins.

- Un argument psychologique peut également être avancé. Dans le monde virtuel, plus encore que dans le monde réel, les consommateurs sont intéressés non par l'engagement de la personne physique derrière un site mais par la personne morale qui en est le responsable.

- Il est pratiquement difficile de lier dans un même certificat une personne physique et la fonction qu'elle exerce, car cette fonction est beaucoup trop dynamique pour qu'on la certifie. Une fonction exercée par X aujourd'hui peut ne plus l'être demain. Ceci pourrait faire peser une charge sur l'A.C. alors que cela relève de la gestion de la personne morale. L'octroi de la signature à une personne morale lui permettrait de maîtriser totalement la gestion de ses clés privées et certificat et donc ses délégations de pouvoir.

- La signature conférée à une personne morale permet à la personne physique de ne pas révéler sauf si la loi exige spécifiquement sa signature en tant qu'individu.

- Enfin, l'attribution d'un certificat aux personnes morales créée une apparence légitime de signature à ces dernières et ce particulièrement dans le chef des destinataires. En d'autres termes, un système de certificat créé des confusions dangereuses.

7. Liberté de choix de signature.

Le développement des nouvelles technologies devrait rapidement généraliser dans un premier temps le recours à la signature digitale et ensuite à d'autres signatures électroniques. Toutefois, les membres de l'atelier estime que l'on ne peut contraindre une personne à recourir à une signature digitale. Le citoyen, en général, et le consommateur en particulier doit toujours garder son libre choix entre sa signature manuscrite et l'usage d'une signature digitale même dans ses rapports avec l'Administration.

Une dérogation à ce principe doit être exceptionnelle et faire l'objet d'un véritable débat public et ne pourrait, en conséquence, le cas échéant être imposée que par une loi.

Dès lors, un membre suggère que dans le projet A.C. agréées soit introduit à l'article 3,§4, premier alinéa, la phrase suivante : « Sauf les exceptions prévues par la loi, nul ne peut-être contraint de recourir à une signature digitale ».

Ce principe semble déjà mis à mal par l'arrêté royal du 22 février 1998 instaurant une déclaration immédiate de l'emploi, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions (M.B. du 18 mars 1998). L'article 3 de cet arrêté royal prévoit que les déclarations d'emploi doivent s'effectuer par voie électronique sauf dérogations. Par voie électronique, il faut comprendre « on line ». Même s'il est vrai que cet arrêté royal a un champ d'application limité et poursuit un but que l'on peut qualifier de légitime

(traquer le travail au noir), les membres de l'atelier estiment qu'il y a risque que ceci fasse tâche d'huile.

8. Imposer un minimum de conditions aux A.C. non-agréées?

Nous avons déjà signalé à plusieurs reprises qu'il pourra coexister sur le marché des A.C agréées et des A.C. non agréées. Le projet actuel ne fixe que des obligations que pour les seules A.C. agréées, dès lors les membres se sont demandés s'il était opportun de prévoir, dans un souci de protection du consommateur, des obligations pour les A.C. non agréées (exemple: contenu minimal d'un certificat, obligation quant à la vérification des informations ou à la révocation,...), tout en sachant qu'une réponse positive à cette question entraînerait une modification du projet de loi.

Après réflexion et échange d'idées, les membres ont estimé cette démarche peu opportune. Selon eux, le but de protection des consommateurs peut être atteint par les législations ou les principes classiques déjà existants, en particulier :

- la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection des consommateurs; l'article 30 de cette loi est notamment mis en exergue :

« Au plus tard au moment de la conclusion de la vente, le vendeur doit apporter de bonne foi au consommateur les informations correctes et utiles relatives au caractéristiques du produit ou du service et aux conditions de vente, compte tenu du besoin d'information exprimé par le consommateur et compte tenu de l'usage déclaré par le consommateur ou raisonnablement prévisible ».

- la jurisprudence sur les obligations essentielles du prestataire; celui qui certifie a au moins une obligation minimale de vérifier l'exactitude de ce qu'il vérifie.

De plus, l'article 22 du projet de loi prévoit des sanctions pénales pour une A.C. qui donnerait l'impression d'avoir la qualité d'A.C. agréée alors qu'elle ne l'est pas.

Notons également qu'une A.C. non agréée qui usurperait cette qualité ou diffuserait des informations laissant croire qu'elle est agréée s'exposerait également à des sanctions sur base de l'article 23 de la loi 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur qui prohibe la publicité trompeuse tant pour les produits que pour les services. Une action en cessation pourrait être intentée également sur base des articles 93 et 94 de cette même loi en raison de pratiques commerciales qui causent préjudice à d'autres vendeurs et aux consommateurs. L'avantage de cette action réside dans le fait qu'elle est formée et instruite selon les formes du référé.

Enfin, il est important de préciser que l'instauration de contrôle sur les A.C. non agréées irait à l'encontre du projet de directive européenne.

Certains membres ont toutefois voulu attirer l'attention sur les problèmes d'interopérabilité. Le projet de loi A.C. agréées impose une obligation d'interopérabilité entre les A.C. agréées, mais les A.C. non agréées n'ont aucune obligation quant à la technique utilisée. Dès lors, certains problèmes pourraient surgir à ce niveau.

9. Protection de la vie privée.

Ce problème a déjà été évoqué antérieurement[21], mais en raison de son importance, il a semblé nécessaire de lui consacrer un point de réflexion particulier.

L'article 7, al. 4 et 5 du projet A.C. agrées disposent :

« Sans préjudice de l'article 5 de la loi du 8 août 1983 relative au registre national, si le certificat est délivré à un titulaire en vue de l'utilisation de la signature digitale dans les échanges avec les autorités publiques, l'autorité de certification vérifie préalablement l'identité du candidat titulaire en consultant le registre national ou d'autres registres désignés par le Roi.
Le Roi fixe les modalités pour l'utilisation de la signature digitale dans les échanges avec les autorités publiques ».

L'article 9 de ce projet dispose, in fine :

« Sans préjudice des articles 8 et 9 de la loi du 8 août 1983 relative au registre national , pour les certificats qui sont délivrés en vue notamment des échanges avec une autorité publique, le registre[22] comporte le numéro d'identification du titulaire au registre national. Ce numéro d'identification ne peut être accessible qu'aux autorités habilitées à l'utiliser ».

L'article 22[23] de ce même projet vise à modifier l'article 5, alinéa premier de la loi du 8 août 1983 relative au registre national pour permettre aux A.C. agréées d'obtenir accès à certaines informations du registre national.

Plusieurs membres se sont posés des questions quant à l'adéquation de ces dispositions avec le droit au respect de la vie privée.

Tel que rédigé l'article 7, alinéa 4 oblige le candidat-titulaire à déclarer l'usage qu'il compte faire de son certificat. En effet, si le certificat va être utilisé dans des relations avec les autorités publiques, il y a obligation pour l'A.C. de vérifier l'identité au registre national. De plus, ne peut-on pas penser que chaque citoyen est susceptible d'utiliser son certificat dans une telle situation. Cela impliquerait une obligation d'office de procéder à une telle vérification. Sinon, si le citoyen n'a pas précisé lors de sa demande de certificat qu'il prévoyait de l'utiliser dans ses rapports avec les autorités pu-

[21] Voir IV.4. Le contenu de certificat et IV.5. Les A.C. sans moyens pour remplir leurs missions?
[22] Il s'agit du registre électronique qui comprend l'ensemble des certificats délivrés par l'A.C.
[23] En fait, cet article dans le projet A.C. agréées est numéroté article 22, en fait il devrait s'agir de l'article 23. Notons également que l'exposé des motifs ne donne aucune explication quant à cet article.

bliques, il devrait demander un nouveau certificat, ce qui représente un coût financier supplémentaire à sa charge, susceptible de freiner l'utilisation de la signature digitale.

Est-il véritablement nécessaire de permettre aux A.C. agréées d'avoir accès au registre national, et ainsi permettre à une société privée, voire à une personne physique de consulter ce registre? Ne serait-il pas préférable de passer par l'intermédiaire d'autorités d'enregistrement qui ont déjà accès au registre national aujourd'hui? Par exemple, une personne souhaitant un certificat pourrait se présenter au service administratif de son Administration communale et se faire délivrer un document qui certifie son identité. Ce document serait remis par le candidat titulaire à l'A.C.. Une telle procédure semble plus respectueuse de la protection de la vie privée.

On peut également se demander comment la disposition de l'article 9, in fine pourra s'appliquer concrètement et correctement. Comment peut-on limiter l'accès au numéro d'identification si celui-ci est publié dans le certificat? L'exposé des motifs est muet quant à cela.

Enfin, il est important de préciser que ces dispositions du projet A.C. agréées sont en contradiction avec l'article 8, second paragraphe du projet de directive européen qui dispose :

> *« Les Etats membres veillent à ce qu'un prestataire de service de certification ne puisse recueillir des données personnelles que directement auprès de la personne qui fait l'objet des données et uniquement dans la mesure où cela est nécessaire à la délivrance d'un certificat ». (nouvelle version).*

Si l'A.C. n'obtient pas les données suffisantes directement de l'intéressé, elle pourrait avoir recours, avec le consentement de l'intéressé, à une autorité d'enregistrement[24] qui a accès au registre national.

, le texte serait alors en adéquation avec les principes élémentaires de protection de la vie privée et avec le texte de projet de directive.

10. Responsabilité et obligations.

10.1. Responsabilités et obligations des A.C. agréées.

Dans ce rapport nous avons longuement abordé les obligations qui incombent A.C. agréées, dès lors nous ne nous attarderons pas sur ce point.

Toutefois, il y a lieu de préciser le régime de responsabilité mis en place par le projet de loi.

L'article 19 traite de la responsabilité des A.C. agréées. Il précise notamment que l'A.C. doit répondre du dommage qui est la conséquence de l'inexécution des obli-

[24] En ce compris le registre national.

gations qui lui sont imposées par ou en vertu de la présente loi. Il appartient au Roi de fixer les montants minimal et maximal en-deçà et au-delà desquels les parties ne peuvent limiter ou étendre la responsabilité de l'autorité de certification.

Il est important de prévoir des règles en matière de responsabilité sous peine de voir le la loi vidée de tout sens et de passer à cotés de deux objectifs essentiels : sécurisation des échanges électroniques et développement du commerce électronique.

Le régime mis en place est fondé sur la présomption simple de responsabilité de l'autorité de certification. Celle-ci pourrait toutefois réfuter cette présomption en démontrant qu'elle s'est conformée aux obligations énoncées dans la loi, ou que le dommage est conséquence d'une faute imputable au titulaire du certificat ou à des circonstances indépendantes de sa volonté.

Lors des travaux, certains membres ont été choqués par le fait que l'on fixe des maxima en matière de responsabilité, d'autres par contre étaient étonnés de l'existence de minima.

10.2. Obligations et responsabilités des titulaires de certificat

L'article 11 prévoit les obligations qui pèsent sur le titulaire d'un certificat :

- il est seul responsable de la confidentialité et de l'intégrité de la clé privée;
- toute utilisation de sa clé privée est réputée, sauf preuve contraire, être de son fait;
- il est tenu dès que nécessaire (doute quant au maintient de confidentialité de la clé privée, perte, vol...) de faire suspendre, voire révoquer son certificat;
- après expiration du certificat ou en cas de révocation ou d'annulation, il ne peut plus utiliser la clé privée correspondante, ni faire certifier la paire des clés par une autre autorité de certification.

L'article 19 prévoit que la responsabilité civile du titulaire est engagée en cas de non respect des obligations légales.

On peut s'étonner de constater qu'il n'existe aucune obligation pour le titulaire du certificat d'informer l'A.C. lorsqu'une donnée figurant dans le certificat est devenue obsolète. Ceci ne pourrait qu'accroître la confiance dans les certificats. Ceci pourrait toutefois être prévu contractuellement.

10.3. Obligations du destinataire du message.

Le texte du projet de loi A.C. agréée prévoit des obligations à charge des A.C. et du titulaire du certificat mais ne dit rien à propos du destinataire du message signé digitalement.

Certains sont d'avis qu'une obligation légale devrait peser également sur le destinataire du message afin de garder un juste équilibre entre les obligations légales de chacune des parties et les responsabilités qui en découlent. Celui-ci devrait au mini-

mum avoir l'obligation de vérifier la signature digitale ainsi que de s'assurer que le certificat n'est ni expiré, ni suspendu, ni révoqué. Les partisans de cette thèse, souhaite que soit inséré la disposition suivante dans le texte légal :

> *« Le destinataire du message signé digitalement est tenu de vérifier la signature digitale au moyen de la clé publique et du certificat émis par une autorité de certification agréée. Le destinataire vérifie également que ce certificat n'est ni expiré, ni suspendu, ni révoqué ».*

Signalons également que dans l'exposé des motifs relatifs à l'article 19, au 8ième paragraphe, page 33, on y lit que l'A.C. pourrait réfuter la présomption de responsabilité en démontrant que le dommage est la conséquence d'une faute imputable au destinataire du message (article 22). Or l'article 22 ne parle nullement du destinataire du message.

D'autres membres estiment qu'une telle obligation légale n'est pas nécessaire au regard de ce qui se pratique dans l'environnement « papier ». La vérification de la signature dans le « monde papier » est uniquement entreprise lorsque le risque le rend nécessaire. On peut imaginer des transactions signées sans risques pour lesquelles le destinataire ne jugera pas utile la vérification de la signature.

11. Le recommandé électronique.

Les membres de l'atelier ont abordé la problématique du recommandé électronique. Il est vrai que dans le « monde réel » un grand nombre d'échanges de courriers se fait par la voie du recommandé postal, notamment dans les échanges avec des autorités publiques.

Ils ont reçu et lu avec grand intérêt une petite documentation relative à la « poste électronique ». Il s'agit d'une initiative canadienne de la société canadienne des postes et de Cebra Inc..

Des discussions, il ressort que le recommandé électronique répond à une véritable attente et doit être au plus tôt légalisé dans le respect de la concurrence. Son absence constitue un véritable frein et obstacle au développement de la société de l'information.

Au cours des travaux, certains membres ont souligné que les pouvoirs publics devaient montrer l'exemple pour favoriser la croissance de la société de l'information. Etant donné que bon nombre de textes légaux font référence à l'usage d'un envoi par recommandé dans les relations avec les pouvoirs publics, une telle action ne saurait que répondre favorablement à cette attente.

A cette fin, un membre propose que soit inséré dans le projet de loi A.C. agréée la disposition suivante :

« Le message signé digitalement basé sur un certificat émis par une autorité de certification agréée dont l'heure, la date, l'envoi, et le cas échéant la réception, sont certifiés par une autorité de certification agréée conformément aux conditions fixées par le Roi constitue un envoi recommandé au sens de l'article 131, 7° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ».

12. Signature électronique valable en matière de sécurité sociale

Au début des travaux, certains membres ont demandé à ce l'on aborde dans le cadre des travaux de l'atelier l'arrêté royal relatif à l'usage de la signature électronique dans la sécurité sociale (banque-carrefour).

Pour répondre à cette demande et compte donné des liens étroits et les implications importantes avec le sujet traité, le professeur Poullet a donné lecture d'un extrait du communiqué de presse du Conseil des Ministres du 11 septembre 1998:

" Le Conseil des Ministres a approuvé, en seconde lecture, après avis du Conseil d'Etat et du Comité de gestion de la Banque Carrefour de la Sécurité Sociale un projet d'arrêté royal relatif à la sécurité sociale. Ce projet introduit un système provisoire de signature électronique. Ce système permettra de signer électroniquement les opérations de déclaration et de communication pour la sécurité sociale.

La signature électronique assure la fiabilité de la communication de données. A défaut, un grand nombre d'informations électroniques devraient être accompagnées de signatures papier.

Ce système provisoire est mis en place pour la période du 1er octobre au 30 juin 1999. Il est introduit en attendant une réglementation juridique globale à propos de la signature électronique. La réglementation provisoire pourra être prolongée par périodes d'un an".

Le texte de l'arrêté a également déposé sur la table par l'un des participants et distribué à l'ensemble des membres. Le texte, assez laconique, a suscité un grand nombre de questions et de réactions.

Les membres regrettent la procédure peu transparente qui a entouré le processus d'élaboration de cet arrêté royal et estiment que l'on essaye déjà de déroger à une loi, alors que celle-ci n'est qu'au stade de projet.

Ils déplorent l'absence de critères devant guider à déterminer les autorités de certification. On ne dispose d'aucune information alors que l'arrêté royal devrait entrer en vigueur le 1 octobre 1998[25]. Le choix des A.C. est laissé à la discrétion de la banque-carrefour. En ce qui concerne les A.C. qui pourraient être retenues, se pose la question de ce qui se passera après l'adoption de la loi relative aux A.C. agréées. Celles-ci ne vont-elles pas bénéficier d'une présomption juris tantum d'être en accord avec

[25] Cet arrêté a été examiné lors de la réunion du 21 septembre 1998, soit 10 jours avant son entrée en vigueur.

l'avant-projet de loi relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales? Que se passera-t-il si après l'adoption de cet avant-projet de loi les autorités de certification agréées par la banque-carrefour ne répondent pas aux conditions légales? Ceci risque de poser des problèmes pour les usagers et avoir des répercussions au niveau de la concurrence.

Des membres se sont également étonnés quant à la procédure juridique employée. Il s'agit d'un arrêté royal qui insère une nouvelle disposition dans une loi, celle du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale. Certes, l'article 38 de la loi du 26 juillet 1996 sur lequel se fonde cet arrêté royal dispose que « le Roi peut, par arrêté délibéré en Conseil des Ministres, prendre toutes les mesures utiles en vue de promouvoir et de régler la collecte par voie électronique (...) ». Mais ceci autorise-t-il le Roi à modifier et compléter une loi. Cette technique semble peu conforme à la hiérarchie des normes et est peu démocratique car implique l'absence de tout débat parlementaire sur cette question.

Certains membres ont demandé si cet arrêté-royal avait été notifié à la Commission européenne conformément à la directive 83/189/CE, telle que récemment modifiée par la directive 98/34/CE, qui prévoit une procédure d'information dans le domaine des normes et réglementations techniques.

Il n'a pas pu être répondu formellement à cette question. D'après certaines informations communiquées à l'atelier la Commission, ayant eu connaissance (soit par la notification ou par une autre voie) de ce texte légal, entend entamer une procédure de suspension.

13. La protection des consommateurs et la signature électronique.

Tout au long des travaux, les membres ont été attentifs aux implications du développement des procédés de signatures électroniques pour les consommateurs. Dans ce rapport figure en filigrane cet intérêt. Toutefois, il semble opportun d'attirer l'attention sur certains points particuliers et de faire part de certaines considérations et propositions exprimées au cours des travaux.

Les avantages que le consommateur peut tirer des innovations technologiques sont indéniables, multiples et divers. Mais en restant objectif et en prenant un regard distant, il faut reconnaître que le développement de la société de l'information et du commerce électronique peuvent présenter certains dangers pour le consommateur.

Pour exemple, le consentement du consommateur peut s'exprimer au moyen d'un simple « clic » en actionnant la souris reliée à un ordinateur.

Il est vrai que l'achat d'un livre ou d'une voiture ne représente pas le même niveau d'engagement pour le consommateur. Les conséquences de l'acte d'achat ne seront pas les mêmes pour le consommateur dans ces deux hypothèses. Dans « le

monde réel » peu de gens lisent intégralement et comprennent les conditions générales d'un contrat. Qui a déjà lu toutes les conditions générales de l'ensemble de ses polices d'assurances? Dans le commerce électronique le consentement du consommateur peut s'exprimer d'une manière plus rapide et les garanties quant à la bonne compréhension de l'acte passé peuvent être moindres.

Les notaires, soutenus par d'autres membres, estiment que les actes authentiques ne peuvent se passer de façon électronique. Ils sont persuadés de la nécessité d'un contact physique, d'un vis-à-vis entre les parties lors de la conclusion d'un tel acte. Le rôle du notaire ne se limite pas à conférer une authenticité à l'acte et à en assurer la conservation, il a également un rôle de conseil et une obligation morale de s'assurer que les parties ont conscience de la portée de l'acte qu'elles signent. Ils ne veulent pas d'un système comme aux Etats Unis. Ce pays ne connaît pas le rôle médiateur du notaire et son apport pacificateur qu'il peut être appelé à jouer. Lors d'un achat immobilier, l'acheteur prend une assurance pour couvrir le dommage qui pourrait résulter de la mise en cause du titre de propriété. Lors de la transaction, l'acheteur n'a aucune garantie quant aux hypothèques ou servitudes liées à ce bien. Ce système s'oppose à la culture européenne basée sur la sécurité juridique des transactions.

Plusieurs membres ont également suggéré que l'on réfléchisse à l'instauration des procédure particulières pour certains actes qui nécessitent une réflexion particulière du consommateur et un certain degré d'engagement financier. Des procédures de doubles signatures peuvent consister en une première solution ou ébauche de solution intéressante.

La fédération des notaires a, quant à elle, émis une proposition concrète en la matière. Celle-ci est apportée afin d'enrichir et est soumise à commentaires dans le but, le cas échéant, de la faire mûrir. Nous proposons au lecteur de prendre connaissance de cette proposition qui suggère l'intégration d'un nouvel article 1334 dans le Code civil, sous le titre « §2. De l'acte sous seing privé » :

> *« La signature d'un écrit sous seing privé ou assimilé à celle-ci peut être légalisée par un notaire lorsque la signature est apposée par le signataire en présence du notaire. Le notaire doit s'assurer préalablement de l'identité de la personne qui a apposé la signature, de la véracité de la signature utilisée par elle et de sa capacité de signer le document.*
> *Le notaire légalise la signature sous seing privé ou assimilée à celle-ci en y apposant la date de la légalisation et sa signature.*
> *De façon identique, un notaire peut légaliser une copie d'un écrit, quelle que soit la technologie utilisée.*
> *La signature ou copie d'un écrit légalisé a la même valeur qu'un acte sous seing privé reconnu conformément à l'article 1322.*
> *La date mentionnée par le notaire vaut en tant que date à l'égard des tiers ».*

Cette disposition créée une nouvelle catégorie d'acte entre l'acte sous seing privé et l'acte authentique. Il s'agit d'un acte qui serait légalisé par le notaire. A l'heure actuelle, la légalisation notariale de la signature est déjà reconnue par les autorités publiques ainsi que par les Cours et Tribunaux dans bon nombre de matières. Des pro-

curations, attestations avec confirmation de l'identité en matière d'adoptions internationales, la légalisation de copies de diplômes, factures ou autres documents légaux, la légalisation de signature sur toutes sortes de formulaires....

La volonté des notaires est de consacrer légalement cette technique de la légalisation notariale, à l'instar de ce qui a été fait par le législateur italien (décret numéro 513 du 10 novembre 1997). La fédération des notaires souhaite également également une réflexion au niveau européen.

La Fédération des notaires constate que dans le monde électronique les parties ne se rencontrent pas de sorte que les contrôles de base, que toute personne effectue, consciemment ou non, lors d'un contact personnel avec une partie contractante, ne sont pas applicables. Il s'agit par exemple d'une appréciation de l'âge (majorité), de la présentation et de la façon d'agir de la partie adverse (santé mentale) et enfin de la connaissance de la portée de la transaction. En d'autres termes, dans le monde électronique, est posée la question pour certains actes de la vérification de la compétence du signataire à s'engager.

Pour répondre à cette incertitude, l'intervention du notaire pourrait garantir l'identité du signataire, sa capacité à s'engager et de sa volonté de signer en toute connaissance de cause.

En cas de légalisation dans le monde électronique, le notaire pourrait apprécier, sous sa propre responsabilité s'il estime nécessaire un contact physique avec le signataire. En effet, dans le but de favoriser le développement du commerce électronique, il pourrait être envisagéde ne pas recourir à un contact physique.

Enfin, la date de la légalisation de l'officier public peut valoir comme date certaine à l'égard de tiers.

Certains membres ont tenu a exprimer des réserves quant à cette proposition. Ces réserves sont de deux ordres. D'une part, certaines personnes estiment que cette proposition est une piste intéressante mais pensent que l'on ne peut réserver cet acte aux seuls notaires.[26] D'autres membres estiment qu'une telle procédure aurait pour conséquence de compliquer les transactions, ce qui va à l'encontre des buts poursuivis par le développement des nouvelles technologies.

Nonobstant, ces réserves, la prise en considération, dans le cadre d'une réglementation protectrice des consommateurs par Monsieur le Vice-Premier Ministre d'une telle proposition instaurant un système non obligatoire de légalisation de signatures valables pour certains types d'actes (ex. : crédit à la consommation est souhaitée. Cette proposition devrait également être relayée auprès du Ministre de la Justice. Nous ne pouvons que conseiller au lecteur de prendre connaissance, en annexe du présent rapport, de la proposition complète et des différentes justifications apportées par la Fédération des Notaires.

[26] En annexe, le lecteur trouvra les arguments avancés par la fédération des notaires pour répondre à cette critique.

14. Signature électronique et service universel.

Si les membres de l'atelier ont estimé nécessaire et indispensable de ne pas obliger le consommateur à recourir à l'usage d'une signature électronique, une majorité d'entre eux estiment nécessaire qu'une étude approfondie sur le service universel dans le cadre de la société de l'information soit menée. Le développement des nouvelles technologies ne doit pas accentuer les écarts sociaux entre les citoyens et priver de l'accès à l'information et au savoir des personnes les plus défavorisées. Dès lors, lorsque dans le futur l'accès à Internet se généralisera, il faudra prendre des mesures pour que chaque citoyen puisse disposer d'une signature électronique.

Il n'y a pas lieu d'attendre que chaque citoyen soit connecté à Internet pour prendre une telle mesure. En effet, Les dispositions et accords pris par les pouvoirs publics belges pour équiper les écoles, bibliothèques et hôpitaux en connexion à Internet constituent un véritable premier pas vers la démocratisation à l'accès pour tous aux réseaux ouverts. De plus en plus, chaque citoyen peut utiliser une connexion à proximité de son domicile. Dès lors, il y a lieu de poursuivre cette volonté de donner la possibilité à tous les citoyens de se connecter à Internet mais tout en réfléchissant aux mesures à prendre pour que chaque citoyen puisse les utiliser de façon efficiente.

15. Légiférer ou attendre.

La volonté politique de légiférer en matière de signature électronique est réelle et répond à une attente exprimée par un grand nombre d'acteurs socio-économiques. Toutefois, nous avons eu à plusieurs fois l'occasion de souligner que la Commission européenne avait également pris une initiative en présentant le 13 mai 1998 une proposition de directive du Parlement Européen et du Conseil sur un cadre commun pour les signatures électroniques.

Dès lors la question essentielle qui se pose actuellement est de savoir s'il y a lieu de retarder les travaux parlementaires relatifs aux deux projets de loi en attendant que la proposition de directive soit adoptée par le Parlement européen et le Conseil et devienne une directive qui devra être transposée en droit interne.

En légiférant maintenant, la Belgique doit s'attendre à devoir revoir, dans le futur, son cadre légal pour l'adapter aux règles européennes.

Il est très difficile de se prononcer sur la durée des travaux européens en la matière. L'adoption de la directive repose sur une procédure de co-décision du Conseil et du Parlement, c'est-à-dire que ces deux organes doivent adopter le même texte. Il s'agit du principe de la navette que nous avons connu très longtemps en Belgique, au

niveau fédéral, lorsque tous les projets et propositions de lois devaient être adoptés par le Sénat et la Chambre avant de pouvoir être sanctionné et promulgué.

A l'heure actuelle, le texte fait l'objet de nombreuses discussions au sein d'un groupe de travail du Conseil. Lorsqu'un accord sera trouvé au sein de ce groupe, le texte sera proposé pour adoption au Conseil. Le texte adopté par le Conseil sera transmis au Parlement. Si le texte est amendé au niveau du Parlement, il retournera au Conseil, et ainsi de suite, jusqu'au moment où les deux instances adopteront le même texte. Signalons pour information et pour exemple, que la procédure relative aux contrats négociés à distance (directive 97/7 de mai 1997) ont duré sept années.

Les avantages que la Belgique pourrait retirer en adoptant une législation rapidement semblent nettement supérieurs aux inconvénients résultant de la nécessité d'adapter ultérieurement ce cadre légal aux normes européennes, dans la mesure où cela donnerait, notamment, un poids plus important dans la négociation, et tenant compte du fait que les principes de base de la directive semblent avoir été fixés.

La suspension des travaux en Belgique constituerait un frein au développement de la société de l'information et du commerce électronique en Belgique étant donné l'absence de sécurité juridique dûment constatée et à la base des initiatives légales dans notre pays.

Toutefois, la poursuite des travaux et le dépôt des deux projets de loi ne doit pas se faire en ignorant les travaux européens. Le texte tel qu'il devrait être prochainement adopté par le Conseil avant transmission au Parlement donnera une première et véritable indication de la tendance européenne. Dès lors, l'Atelier estime nécessaire qu'une étude soit réalisée dès l'adoption du texte par le Conseil et qu'un rapport soit fait aux Ministres de l'Economie et de la Justice à l'attention des Parlementaires belges. Cette étude devrait clairement mettre en évidence les points de divergences entre le texte européen et les projets fédéraux. De ce fait, lors des travaux parlementaires belges, le projet de loi pourrait être adapté sur les points faisant l'objet d'un consensus européen.

Signalons que d'autre pays européens (ex. : Luxembourg, Autriche, Irlande et probablement la France) s'apprêtent à se doter d'un cadre légal en matière de signature électronique nonobstant les travaux européens. Dès lors, l'attente pourrait conduire à l'isolement de notre pays.

Ce vendredi 27 novembre 1998, la proposition de directive a été soumise au Conseil « Télécoms ». Les Ministres n'ont pas adopté ce texte. Le point fondamental qui a donné lieu à cet échec est le suivant : l'annexe III proposée, qui était à l'origine relative aux exigences pour les dispositifs de création et de vérification des signatures électroniques, et qui est devenue à la suite d'un compromis, relative uniquement aux exigences pour les dispositifs de création de signatures électroniques, doit-elle être obligatoire pour admettre les effets juridiques des signatures de l'article 5,1 ou doit-elle être facultative?

D'une part, le Royaume-Uni, l'Irlande, l'Espagne, les Pays-Bas, les pays nordiques (sauf le Danemark, plus ou moins neutre), le Luxembourg et la Grèce, soutenus

par la Commission, souhaitent l'optionalité, et donc un niveau de sécurité de sécurité inférieur, sous prétexte de l'impossibilité de contrôler dans la pratique, tous les points de l'annexe III; de plus, ces pays estiment que le marché risque d'en souffrir, et qu'il y a lieu de se rapprocher des approches américaine et japonaise qui prônent la liberté et la « self-regulation ».

D'autre part, la France en tête, l'Allemagne, l'Italie (très ferme sur sa position), le Portugal, la Belgique (plus souple et favorable à un compromis), qui souhaitent avoir un minimum d'exigences obligatoires reprises dans l'Annexe III pour pouvoir accorder l'effet juridique de l'article 5.1. aux signatures.

C'est donc un problème de sécurité au niveau « utilisateur » (hardware et software) et le problème de la protection des clés privées (peut-elle être copiée ou non sur le disque dur de l'utilisateur ?) qui sont à l'origine d'une divergence fondamentale. Il ne sert à rien de changer les mots si les concepts ne peuvent se rejoindre.

16. Suggestion de pistes de prolongation.

Les deux projets de textes légaux constituent une étape importante pour la Belgique dans son passage vers la société de l'information. L'adoption de ces projets sera un pas encore plus significatif, mais ne constituera pas une fin. Lors des travaux, certains membres ont tenu à préciser qu'il était nécessaire de poursuivre la réflexion sur certains points :

- article 1325 du Code civil qui impose le double original pour les contrats synallagmatiques;

- articles 1326 et 1327 du Code civil qui prévoit la mention manuscrite de la valeur en chiffres et en lettres pour la promesse unilatérale;

- article 1328 du Code civil : date certaine

- les problèmes liés à la conservation des clés et à l'archivage.

V. RECOMMANDATIONS

PREALABLES

1. L'atelier exprime l'urgence de donner un cadre légal à la signature électronique

2. Il s'agirait par là

- d'affirmer l'équivalence de la signature électronique à la signature manuscrite pour autant que la première réponde aux exigences fonctionnelles de la seconde et présente dès lors la sécurité requise.

- d'affirmer le principe de neutralité technologique, à savoir que cette équivalence fonctionnelle peut être rencontrée par diverses techniques qu'il s'agisse de la reconnaissance de caractéristiques biométriques (reconnaissance dynamique de la signature ou de l'iris, ...), de la cryptographie symétrique ou asymétrique même si cette dernière technologie peut être à court terme privilégiée.

- Lorsque la technologie de la cryptographie asymétrique à clef publique est utilisée, de reconnaître cette équivalence à des signatures certifiées par certaines autorités moyennant des conditions réglementaires précises qui seront développées ci-dessus ;

3. L'atelier se réjouit de voir que ce double objectif est rencontré (nonobstant certaines critiques reprises ci-après) par les deux avants-projets de loi présentés par les Ministres de la Justice et des Affaires économiques et souhaite dès lors les voir aboutir sous peu.

4. L'atelier estime qu'il n'y a pas lieu de retarder les travaux parlementaires belges en attendant l'adoption de la directive européenne. Une telle attitude ne saurait que ralentir le développement de la société de l'information et du commerce électronique en Belgique. Les avantages de l'adoption d'un cadre réglementaire sont nettement supérieurs aux inconvénients d'une éventuelle adaptation de ce cadre lorsque la directive sera promulguée au Journal Officiel des Communautés européennes. Toutefois, l'atelier recommande qu'une étude soit menée lors de l'adoption du texte par le Conseil afin de faire rapport aux Ministres concernés et au Parlement des adaptations nécessaires à apporter aux projets.

CARACTERISTIQUES D'UNE LEGISLATION EN MATIERE D'AUTORITES DE CERTIFICATION

1. On veillera à ce que les critères fixés pour l'agrément soient minimaux (notamment en matière de responsabilité, normalisation, contenu de certificats, ...) de manière à favoriser au maximum la concurrence sur ces divers points.

2. Il importe que des critères clairs et transparents existent pour l'agrément des autorités de certification. Cette exigence n'est pas rencontrée par la réglementation provisoire prise en matière de sécurité sociale. L'atelier suggère que chaque exigence réglementaire n'excède pas ce qui est strictement nécessaire à assurer le respect des exigences de sécurité du commerce électronique.(ex : protection de la vie privée)

3. La législation mais surtout les règlements d'application de cette législation se conformeront dans toute la mesure du possible aux standards internationaux, de manière à garantir une parfaite interopérabilité des certificats nationaux, européens et de pays tiers.

4. Dans une matière caractérisée par une grande évolutivité, des mécanismes garantissant une grande souplesse c'est-à-dire la possibilité d'adaptation des normes en fonction de l'évolution technologique sont requis.

5. Enfin, la réglementation proposée doit être pleinement respectueuse des libertés des individus, en particulier des règles en matière de protection des données, celles relatives au droit de ne pas se voir imposer des procédures de signature électronique et à l'inverse, du droit dans le futur lorsque se généralisera l'accès à Internet, de droit de chaque citoyen de disposer d'une signature électronique.

6. En matière des personnes morales, la valeur légale de la reconnaissance des signatures électroniques des personnes morales ne doit pas être exclue.

PROLONGATIONS SUGGEREES RELATIVES A LA SIGNATURE DE CERTAINS ACTES

Si la réglementation en projet est jugée satisfaisante pour la majorité des actes, l'Atelier a cependant émis quelques suggestions :

1. en matière d'actes authentiques : il a pris acte de la volonté des notaires de ne pas modifier le principe du face à face entre le notaire instrumentant et la ou les personne(s) parties à l'acte authentique

2. L'atelier souhaite que pour la conclusion de certains actes exigeant une réflexion du consommateur, des procédures de double signature puissent être offertes voire imposées, soit par l'intervention d'un tiers (cfr. la proposition des notaires), soit par l'obligation d'une signature apposée sur des mentions spécifiques de l'acte, outre la signature globale de l'acte.

3. L'atelier souhaite que les procédures du double (1325 CC) et de date certaine (1328 CC) puissent être réalisées électroniquement.

4. Le recommandé doit pouvoir être réalisé par voie électronique et ce dans le respect du droit de la concurrence.

Bruxelles, le 16 décembre 1998.

5. Les problèmes liés à l'archivage et à la conservation des clés méritent une attention particulière, dans la mesure où l'évolution technologique risque d'une part d'insécuriser certaines clés et, d'autre part, de ne plus pouvoir les régénérer ou conserver la trace fiable de l'émetteur.

6. En matière de dispositifs de création de signature électronique, il faudra déterminer un juste compromis entre d'une part les dispositifs de sécurité pour l'utilisateur et d'autre part le minimum d'entraves au développement technologique.

7. l'Atelier souhaite que la réflexion soit approfondie sur certains points de ce rapport et, notamment, sur la nécessité ou non d'imposer des conditions minimales aux A.C. non agréées.

8. Enfin, l'atelier suggère que les différents Ministres, et plus particulièrement le Ministre de l'Economie en collaboration avec son collègue ayant en charge la fonction publique, chargent leurs administrations d'examiner les différents textes légaux afin de s'assurer que les échanges entre administrations et administrés puissent se faire de façon électronique tant du point de vue légale que du point de vue pratique. Les membres soulignent également l'importance des travaux des S.S.T.C. (projet Agora) et demandent à ce qu'ils se poursuivent.

PARTIE II : LA LABELLISATION DE SITES

I. INTRODUCTION

Le commerce électronique est une forme de vente à distance mais, force est de reconnaître, qu'il présente des particularités propres et que dès lors il se singularise par rapport aux formes traditionnelles de vente à distance.

Vous voilà, vous consommateur, sur Internet occuper à surfer sur le *web*. Vous voici sur un site et dénichez un produit intéressant; vous souhaitez l'acheter, cependant des doutes sont toujours présents en vous, ils traduisent une multitude d'interrogations : qui est donc ce vendeur, existe-t-il réellement, le produit vu à l'écran correspond-il à celui que je vais obtenir, puis-je communiquer mes données personnelles sur le réseau et mon numéro de carte de crédit, que se passera-t-il en cas de problème, le vendeur dispose-t-il d'un service après-vente, un droit de rétractation me bénéficie-t-il comme la loi le prévoit dans le cadre des ventes à distance?

Ces questions sont bien réelles, elles ne font que traduire les craintes exprimées par les consommateurs et mises en relief dans différentes études réalisées à travers le monde. Ainsi en Belgique, le Centre de Recherche et d'Information des Organisations de Consommateurs (CRIOC) vient de réaliser une enquête.

« Il apparaît que 35% de 1,5 Million d'utilisateurs d'Internet recensés en Belgique n'ont, en fait, aucune confiance dans l'achat de biens et services via ce réseau et 19% déclare ne pas marquer d'intérêt pour cette forme de commerce. Les optimistes sont 11% : ils ont eux, franchi le pas et acheté au moins une fois sur Internet. Ce qui retient les autres? Pour 57% des surfeurs c'est l'insécurité tant en ce qui concerne le bien ou le service que l'identité du vendeur et le moyen de paiement. 45% des sondés sont convaincus qu'ils n'auront pas recours à Internet pour l'achat de quoi que ce soit, 24% émettent des doutes et 31% n'excluent pas, a priori, cette possibilité ».[27]

Ces chiffres sont révélateurs des craintes exprimées par les consommateurs belges. Mais il ne s'agit pas de chiffres isolés, les tendances sont les mêmes dans les différents pays.

Cela signifie-t-il qu'il est dangereux et téméraire d'effectuer ses achats sur Internet? Non, les moyens techniques actuelles permettent de sécuriser les transactions, mais tous les vendeurs ne disposent pas nécessairement d'équipements techniques adéquats.

[27] « Acheter sur Internet », le Vif-l'Express, Louis Brouhal, 2/10/98

Les chiffres de l'étude du CRIOC mettent en évidence trois catégories d'internautes : ceux qui participent au commerce électronique, les indécis et enfin ceux qui affirment ne pas vouloir de cette forme de commerce. Une étude représente une situation à un moment donné. Des actions positives peuvent faire évoluer ces chiffres. Que peut-on faire pour convaincre les indécis et pour faire prendre conscience aux derniers des avantages et du potentiel élevé du commerce électronique?

L'utilisation combinée des technologies et de l'audit permet de répondre à l'inquiétude exprimée par les consommateurs. La certification de site, ou labellisation de site, est la procédure qui non seulement par des méthodes classiques d'audit, permet, en effet, d'évaluer soit un point particulier (la sécurité, la protection de la vie privée, la protection des consommateurs,...) soit de manière plus globale la qualité des sites, mais en outre, par des procédures de page écran, des hyperliens avec les certificats des auditeurs et des labels téléchargés par les auditeurs créent la possibilité pour les internautes de prendre connaissance de l'octroi d'un label comme de son retrait.

La labellisation apparaît comme une technique qui peut rencontrer les aspirations des consommateurs et des professionnels.

Les travaux de l'atelier se sont penchés sur cette piste qui a été examinée au regard d'exemples étrangers et d'un projet belge. Les membres de l'atelier ont ensuite réfléchi aux implications, conséquences et conditions nécessaires à l'installation d'une telle procédure en Belgique. Enfin, ils émettent des recommandations précises, qu'ils estiment nécessaires d'être rencontrées pour que la certification de site devienne effective et efficace dans notre pays.

II. PRESENTATION D'UNE INITIATIVE ETRANGERE - *WEBTRUST*[28]

La labellisation de sites Internet existent déjà, ce concept a été développé en Amérique. Il semble utile pour la bonne compréhension de présenter une initiative étrangère afin de mieux cerner la portée de cette procédure de labellisation. Nous vous proposons de prendre connaissance des labels « *webtrust* » et « truste ». Seul le premier de ces deux labels sera présenté d'une manière exhaustive.

1. Introduction

Le 16 septembre 1997, l'Institut Canadien des Comptables Agréés (ICCA) et l'American Institute of Certified Public Accountants (AICPA) ont annoncé la création d'un sceau de certification pour le commerce électronique baptisé *Webtrust*. Cette initiative a été mise sur pied dans le but d'essayer de développer le commerce électronique entre entreprises et consommateurs.

De différentes enquêtes menées concluant au manque de confiance des consommateurs à participer au commerce électronique l'AICPA a identifié trois grands secteurs de risques associés au commerce électronique : les pratiques commerciales, l'intégrité des opérations et la protection de l'information.

Les pratiques commerciales : Le commerce électronique suppose souvent des opérations entre des partenaires inconnus. Les apparences peuvent être trompeuses : comment le consommateur peut-il être sûr que les biens et services présentés de façon attrayante dans une page *web* seront livrés tels quels par le vendeur qui les offre? Comment le consommateur peut-il savoir si le vendeur accepte le retour d'articles vendus ou si ces articles sont garantis? Etant donné le caractère anonyme du commerce électronique et la facilité avec laquelle les personnes malhonnêtes peuvent établir, puis abandonner, une identité virtuelle, il est essentiel que les consommateurs sachent que les entités avec lesquelles ils font affaire déclarent leurs pratiques commerciales et les respectent. Sans ces renseignements utiles et sans l'assurance que l'entité a respecté dans le passé les pratiques déclarées, les consommateurs courraient un risque accru de subir des pertes, d'être victimes d'une fraude, d'éprouver des contrariétés ou de voir leurs attentes déçues.

Intégrité des opérations : Sans des contrôles adéquats, les opérations et les documents électroniques peuvent être aisément modifiés, perdus ou reproduits et faire l'objet d'erreurs de traitement. L'intégrité des opérations et des documents électroniques risque alors d'être mise en cause, ce qui pourrait provoquer des conflits au sujet des conditions de l'opération et de la facturation. Il est donc normal que les personnes qui envisagent d'avoir recours au commerce électronique cherchent à obtenir l'assurance que l'entité a mis en place des contrôles efficaces sur l'intégrité des opéra-

[28] Cette présentation reproduit les informations trouvées sur le site de l'Institut Canadien des Comptables agréés : http//www.icca.ca

tions, qu'elle a, dans le passé, traité les opérations de façon précise, complète et rapide, et qu'elle a facturé ses clients conformément aux sommes convenues.

Protection de l'information *(Privacy)*: Il importe donc que les consommateurs soient persuadés que le site *Web* qu'ils consultent est identifié de manière adéquate et que l'entité a pris les mesures voulues pour protéger la confidentialité des données personnelles des clients. Bien qu'il soit relativement facile de créer un site *Web* dans Internet, la technologie nécessaire est souvent complexe et pose toute une série de problèmes touchant à la protection des données et aux questions de sécurité qui s'y rattachent. La confidentialité des données de nature délicate transmis par Internet peut se trouver compromise. Par exemple, sans le recours à des techniques de chiffrement élémentaires, les numéros de carte de crédit des consommateurs pourraient être interceptés pendant la transmission et volés. De même, en l'absence de coupe-feu et d'autres mesures de sécurité, des renseignements personnels d'un client qui se trouvent sur le système informatique de commerce électronique d'une entité pourraient être, délibérément ou non, mis à la disposition d'un tiers non lié aux activités de l'entité. Les entorses à la sécurité peuvent également comprendre l'accès non autorisé à des réseaux d'entreprises, à des serveurs Internet/*Web* et même à la connexion Internet du consommateur (par exemple, son ordinateur à la maison). Il est donc normal que les personnes qui envisagent d'avoir recours au commerce électronique cherchent à obtenir l'assurance que l'entité a mis en place des contrôles efficaces sur la protection de l'information et qu'elle a, dans le passé, protégé la confidentialité des données personnelles des clients.

2. Le sceau de certification *webtrust*

Le *Web* a retenu l'attention des entreprises et des consommateurs, de sorte que le nombre et les types d'opérations électroniques se sont accrus rapidement. Pourtant, beaucoup sont d'avis que le commerce électronique atteindra son plein potentiel seulement lorsque les consommateurs auront l'impression que les risques associés aux opérations commerciales électroniques sont réduits à un niveau acceptable. Les inquiétudes des consommateurs quant à l'intégrité, au contrôle, à l'autorisation, à la confidentialité et au caractère anonyme des opérations sont souvent légitimes. Dans un univers où l'interlocuteur demeure invisible, chacun a besoin d'obtenir une assurance d'une tierce partie objective. Cette assurance peut être fournie par un comptable agréé («CA») ou par un certified public accountant («CPA») indépendant et objectif, et constatée par l'affichage d'un sceau de certification *Webtrust* dans le site *Web*.

Le sceau de certification *Webtrust* symbolise, pour les clients éventuels, le fait qu'un CA ou un CPA a évalué les pratiques commerciales et les contrôles du site *Web* afin de déterminer s'ils sont conformes aux «Principes et critères *Webtrust*» pour le commerce électronique entre entreprises et consommateurs, et qu'il a délivré un rapport dans lequel il formule une opinion sans réserve indiquant que les principes sont respectés au regard des critères *Webtrust*. À ce sujet, voir l'Annexe A[29], «Exemples de rapports de praticiens». Les principes et critères reflètent des normes fondamentales en matière de

[29] Voir Annexes au Rapport - Annexe n°7

transparence des pratiques commerciales, d'intégrité des opérations et de protection de l'information.

3. Le C.A. et le C.P.A. : des professionnels de la certification.

Les CA et les CPA offrent des services de certification. Leur rôle est de fournir une assurance au lecteur ou utilisateur, la plus connue étant celle qui résulte d'une vérification d'états financiers. On accorde de la valeur à une opinion de vérificateur signée par un CA ou un CPA parce que ces professionnels ont de l'expérience en matière de certification et de comptabilité financière et qu'ils sont reconnus pour leur indépendance, leur intégrité, leur discrétion et leur objectivité. En outre, les CA et les CPA se conforment à un ensemble complet de règles de déontologie et de normes professionnelles dans la prestation de leurs services.

Toutefois, l'assurance fournie relativement à des états financiers n'est qu'un seul des types de service de certification que peuvent offrir les CA et les CPA. Ils sont également appelés à procurer une assurance en matière de contrôle interne et en ce qui concerne la conformité de certains éléments avec des critères déterminés. L'expérience professionnelle, l'expérience du monde des affaires, la connaissance approfondie du domaine (sécurité, vérifiabilité et contrôle des systèmes de commerce électronique) et les caractéristiques professionnelles (indépendance, intégrité, discrétion et objectivité) nécessaires dans le cadre de telles missions sont aussi les éléments clés qui permettent à un CA ou à un CPA d'évaluer de manière exhaustive et objective les risques, les contrôles et les informations sur les pratiques suivies qui sont associés au commerce électronique.

4. Obtention et conservation du sceau de certification *webtrust.*

Le processus de certification

La direction de l'entité fait au praticien une déclaration (des assertions) qui pourrait ressembler à la suivante :

Dans son site *Web* consacré au commerce électronique (à l'adresse www.abc.com), la société ABC :

- a indiqué les pratiques qu'elle a adoptées pour ses opérations de commerce électronique et a effectué ses opérations conformément à ces pratiques,
- a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les commandes passées par le client par la voie du commerce électronique ont été traitées et facturées comme convenu,
- a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les renseignements personnels du client obtenus dans le cadre d'une opération de commerce électronique sont protégés contre toute utilisation étrangère aux activités de ABC,

pour la période allant du JOUR MOIS 199X au JOUR MOIS 199Y, en conformité avec les critères *Webtrust* établis conjointement par l'ICCA et l'AICPA.

Dans le cas d'une déclaration initiale, la durée de la période couverte devrait être d'au moins deux mois et sera normalement de trois mois ou plus selon ce que déterminera le praticien. Dans le cas des déclarations ultérieures, la période couverte devrait avoir comme point de départ la fin de la période précédente, de manière à éviter toute solution de continuité entre deux déclarations.

Pour que la déclaration soit fondée, la direction de l'entité doit s'être dotée d'une structure de contrôle interne appropriée pour ses opérations de commerce électronique. On peut trouver des indications utiles à cet égard dans les publications du Conseil sur les critères de contrôle (CCC) au Canada, ou dans celles du Committee of Sponsoring Organizations (COSO) de la Treadway Commission aux États-Unis. Toutefois, pour les besoins de la délivrance du sceau de certification *Webtrust*, le praticien n'évalue que les éléments du contrôle interne qui sont pertinents par rapport au traitement des opérations de commerce électronique.

Un praticien indépendant, objectif et bien informé contrôle par sondages la validité d'une telle déclaration en se fondant sur les normes professionnelles de l'ICCA ou de l'AICPA, et fournit une opinion professionnelle qui ajoute à la crédibilité des déclarations de la direction de l'entité.

Obtention du sceau

Pour obtenir le sceau de certification *Webtrust*, l'entité doit respecter tous les principes *Webtrust*. L'évaluation se fait par référence aux critères *Webtrust* associés à chacun de ces principes. De plus, l'entité doit :
1) faire appel à un CA ou à un CPA à qui l'ICCA ou l'AICPA a expressément délivré un permis autorisant la prestation du service *Webtrust*;
2) obtenir un rapport sans réserve de ce praticien. Le questionnaire d'auto-évaluation présenté à l'Annexe B[30], devrait aider la direction de l'entité à établir le bien-fondé de ses assertions.

Conservation du sceau

Une fois le sceau obtenu, l'entité peut continuer de l'afficher dans son site *Web* si les conditions suivantes sont remplies :

Le praticien met périodiquement à jour sa certification de la déclaration. L'intervalle entre les mises à jour est fonction d'éléments tels que les suivants :
- la nature et la complexité des activités de l'entité;
- la fréquence des changements importants apportés au site *Web*;

[30] Voir Annexes au Rapport - Annexe n°7

- l'efficacité relative des contrôles de surveillance et de gestion des changements que l'entité a mis en place pour assurer le respect continu des critères *Webtrust* chaque fois que des changements sont apportés au site *Web*;
- le jugement professionnel du praticien.

Par exemple, les mises à jour seront plus fréquentes dans le cas du site *Web* en constante évolution d'une institution financière dans lequel s'effectuent des opérations sur des titres que dans le cas d'un service en ligne qui vend des données d'archives dans un site *Web* rarement modifié. Dans tous les cas, l'intervalle séparant deux mises à jour ne saurait excéder trois mois, mais il sera souvent considérablement plus court.

L'entité s'engage à informer le praticien, entre deux mises à jour, de tous les changements importants apportés à ses politiques commerciales, à ses pratiques, à ses processus et à ses contrôles dans la mesure où ces changements sont susceptibles d'influer sur la capacité de l'entité de continuer à respecter les «Principes et critères *Webtrust*», ou sur la manière dont ils sont respectés. En cas de tels changements, il pourrait s'avérer nécessaire de procéder à une mise à jour de la certification ou, dans certaines situations, au retrait du sceau jusqu'à ce qu'une vérification de mise à jour soit possible. Lorsque le praticien découvre qu'un tel changement s'est produit, il détermine s'il doit effectuer une vérification de mise à jour et s'il s'avère nécessaire de retirer le sceau de certification jusqu'à l'achèvement de la vérification de mise à jour et la délivrance du rapport de vérificateur mis à jour.

Processus de gestion du sceau

Le sceau de certification *Webtrust* est géré par un tiers, soit un organisme de service de confiance (le «gestionnaire de sceau»), selon les lignes directrices suivantes :

- Il est nécessaire que l'entité demande et obtienne un certificat spécial de catégorie 3 (special Class 3 Certificate) – soit le certificat numérique *Webtrust* – du gestionnaire de sceau.
-Si l'entité reçoit un rapport sans réserve, le praticien avise le gestionnaire de sceau que le sceau peut être affiché sur le site *Web* de l'entité, avec une identification numérique précise, et fournit une date d'expiration.
-De plus, le praticien ou le gestionnaire de sceau fournit un applet (mini-application informatique utilisée sur le *Web*) à l'entité. L'applet indique à la page *Web* de communiquer avec le gestionnaire de sceau et, si l'autorisation a été accordée, d'afficher le sceau et les liens hypertextes associés au rapport du praticien et à toute autre information pertinente. Le gestionnaire de sceau fournit également un certificat numérique spécial *Webtrust* à l'entité.
-Si, pour une raison valable, le praticien décide que le sceau doit être retiré du site *Web* de l'entité, il en avise l'entité et demande que le sceau et le rapport connexe du praticien soient retirés du site *Web*. Le praticien envoie aussi un avis de révocation de l'autorisation d'affichage du sceau au gestionnaire de sceau, ce qui entraîne la révocation électronique du sceau et empêche l'entité de continuer à l'afficher.

-A moins qu'un avis de mise à jour ne soit reçu, l'autorisation d'afficher le sceau prend fin, le site *Web* se voit demander de retirer le sceau et le rapport du praticien, et le gestionnaire de sceau retire l'autorisation d'afficher le sceau à compter de la date d'expiration.

Authentification du sceau

Pour vérifier l'authenticité d'un sceau affiché dans un site *Web*, le client peut cliquer sur le sceau afin de faire apparaître une représentation graphique d'un certificat. Ce certificat graphique indique au client comment procéder pour visualiser, à l'aide de son navigateur, le certificat numérique spécial *Webtrust* attribué par le gestionnaire de sceau. Ce certificat numérique fournit au client une preuve de la validité du sceau *Webtrust*. Il indique qui a délivré le certificat, à qui le certificat a été délivré, et comment entrer en communication avec l'entreprise à qui le certificat a été accordé. En l'absence de ce certificat numérique, le sceau *Webtrust* ne doit pas être considéré comme valide.

5. Les principes *webtrust.*

Transparence des pratiques commerciales.

L'entité indique ses pratiques en matière de commerce électronique et effectue ses opérations conformément à ces pratiques.

Pour accroître la confiance du consommateur à l'égard du commerce électronique, il importe que le consommateur soit informé des pratiques commerciales suivies par l'entité dans le cadre de ses opérations de commerce électronique. Par conséquent, l'entité doit indiquer convenablement ses pratiques concernant des éléments comme les commandes, les retours éventuels et les réclamations au titre d'une garantie; en outre, l'entité doit effectuer ses opérations conformément à ces pratiques. Ce principe a trait à la façon normale d'agir de l'entité en matière de commerce électronique. Il ne concerne d'aucune manière la qualité des biens ou des services, ou leur pertinence par rapport aux besoins du consommateur.

Intégrité des opérations.

L'entité a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les commandes passées par le client par la voie du commerce électronique sont traitées et facturées comme convenu.

Ces contrôles et pratiques ont notamment trait aux aspects suivants des opérations : identification appropriée de l'opération; validation de l'opération; exactitude, exhaustivité et rapidité du traitement de l'opération et des facturations y afférentes; indication des modalités de l'opération et de la facturation et, le cas échéant, du règlement électronique. Il s'agit de points importants pour gagner la confiance des consommateurs à l'égard du commerce électronique.

Protection de l'information

L'entité a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les renseignements personnels du client obtenus dans le cadre d'une opération de commerce électronique sont protégés contre toute utilisation étrangère aux activités de l'entité.

Ces contrôles et pratiques ont notamment trait au chiffrement ou à d'autres modes de protection des renseignements personnels du client (numéros de carte de crédit ou données personnelles et financières) transmis à l'entité par l'entremise d'Internet, à la protection de ces renseignements une fois qu'ils ont été reçus par l'entité, et à l'obtention de la permission du client pour utiliser l'information dans un but autre que celui lié aux activités de l'entité, ou pour stocker, modifier ou copier des données provenant de l'ordinateur du client. L'inquiétude des consommateurs au sujet de la protection des renseignements personnels a été jusqu'ici l'un des principaux facteurs de dissuasion à la conclusion d'opérations de commerce électronique.

6. Les critères *webtrust*

Les critères *Webtrust* ont été élaborés afin de fournir des indications plus précises au sujet du respect des principes *Webtrust*. Ces critères constituent une base de référence au regard de laquelle une entité peut faire une auto-évaluation de la façon dont elle se conforme aux principes; il s'agit en outre d'un ensemble cohérent de critères de mesure applicables par les praticiens aux fins de l'essai et de l'évaluation des sites *Web*.

Une disposition sur deux colonnes a été utilisée pour présenter les critères. La première colonne présente les critères en tant que tels, c'est-à-dire les conditions auxquelles l'entité doit répondre pour être en mesure de démontrer que le principe a été respecté. La deuxième colonne fournit des exemples d'informations et de contrôles. Il s'agit d'exemples d'informations que l'entité peut fournir ou de contrôles qu'elle a pu mettre en place afin de se conformer aux critères. Des informations et contrôles différents ou supplémentaires peuvent également être valables.

L'entité doit être en mesure de démontrer que, sur une période d'au moins deux mois ou, généralement, de trois mois ou plus :
1) elle a réellement effectué ses opérations conformément aux pratiques de commerce électronique indiquées;
2) ses contrôles ont fonctionné efficacement;
3) elle avait en place un environnement de contrôle propice à la communication d'informations fiables sur ses pratiques commerciales et à l'application de contrôles efficaces; et
4) elle avait en place des procédures de surveillance permettant d'assurer que les pratiques commerciales indiquées sont toujours suivies et que ses contrôles continuent d'être efficaces. Ces notions constituent une partie intégrante des critères *Webtrust*.

III. Présentation de projets belges.[31]

Ces initiatives étrangères n'ont pas laissé insensibles certaines sociétés belges. En effet, Belsign associé à Coopers&Lybrand ont mis sur pied un projet, dont le but est d'octroyer un label baptisé « trust 2 ».

En lien avec ce premier projet mais de manière autonome, l'Institut des Réviseurs d'Entreprises a également initié une réflexion à propos des conditions dans lesquelles les réviseurs d'entreprises pourraient délivrer des sceaux aux entreprises qui offrent des produits ou des services par l'intermédiaire de leur site Internet.

Projet de l'Institut des Réviseurs d'Entreprises.

Ce sceau de qualité n'est délivré qu'aux commerçants qui satisfont strictement à un certain nombre de normes préétablies. L'assurance qu'un commerçant respecte ces normes est obtenue par le biais d'un audit périodique, couvrant les domaines suivants :

- Organisation et compétence : l'audit veille à s'assurer que la structure d'organisation et du personnel permette au commerçant de garantir une maîtrise correcte des opérations, par exemple : l'allocation précise des responsabilités, les compétences du commerçant,...

- Mode de fonctionnement : vérification est faite quant aux mesures mises en oeuvre pour garantir l'intégrité de la transaction. Cela se traduit par exemple par des exigences précises en matière d'information au consommateur : description des produits, affichage des prix, conditions de vente et de paiement, confirmation et/ou annulation des commandes, conditions et frais de livraison, services après-vente, traitement des plaintes éventuelles,...

- Législation et fiscalité : L'audit examine la façon dont le commerçant respecte des dispositions légales et fiscales : loi sur les pratiques du commerce, protection de la vie privée, code de la T.V.A.,....

- la sécurité : le commerçant dispose-t-il des moyens techniques et organisationnels qui lui permettent de garantir la disponibilité de son site *web*, l'intégrité des logiciels utilisés, la confidentialité et la protection des données échangées (exemple : les mesures de backup, la configuration du firewall et le niveau de protection contre les intrusions,...).

[31]. Cette présentation est basée sur les éléments apportés oralement par les initiateurs du projet au membres de l'atelier et des informations se trouvant sur le site de la société Belsign (http://www.belsign.be). Au moment des travaux et de l'élaboration de ce rapport, les membres n'ont pas connaissance d'une autre initiative que celle présentée. Dès lors, c'est pour être complet que ce projet est présenté, il ne s'agit pas d'une volonté des membres de privilégier cette initiative au détriment d'une éventuelle autre. D'ailleurs les membres recommandent que la labellisation se fasse dans un marché concurrentiel. On note que récemment, l'Association belge du Marketing Direct a adapté en même temps qu'un code de déontologie, un lable de confirmité à ce même code, pour les entreprises membres de l'association. Pour le moment, ce label ne vise que les activités traditionnelles et non les autorités en ligne.

Le programme d'audit développé par l'IRE se base sur un questionnaire qui comprend environ 200 questions qui couvrent les différents aspects susmentionnés. Ce questionnaire est un guide pour l'auditeur, il n'appartient pas celui-ci de répondre à toutes les questions. Dans le cadre du présent projet, l'audit serait confiée à un réviseur d'entreprise. L'auditeur après l'examen du site rendra un rapport. Si celui-ci laisse apparaître que le commerçant satisfait aux normes, une opinion d'audit des alors émise, qui résume les résultats de l'enquête. C'est uniquement à l'issue d'une enquête positive que le sceau de qualité est décerné par l'auditeur, sous la forme d'un icône qui figurera sur la home page du site. Chaque utilisateur de ce site peut donc s'assurer en un coup d'oeil que le commerçant virtuel est fiable. Par ailleurs, le rapport d'audit peut être consulté en cliquant simplement sur l'icône, tout comme peuvent être visualisées les normes sur lesquelles cet audit a été basé.

Ce sceau sera également repris dans le certificat digital délivré par une autorité de certification agréée par l'Etat belge (dans la mesure où une législation est adoptée en la matière).La technologie cryptographique utilisée à cet effet assure de l'authenticité de l'icône apposé sur le site. Par le même biais, l'autorité de certification confirme l'identité du commerçant. Les certificats digitaux qui confirment l'identité d'une personne (morale) sont déjà délivrés par l'autorité de certification. Des procédures approfondies de vérification d'identité garantissent au visiteur du site *web* qu'il a bien atteint le site déterminé qu'il cherchait à joindre. Qui plus est, ce sceau permet au commerçant de garantir la confidentialité des transactions qui transitent par son site. L'apposition du sceau sur le certificat digital lui apporte une valeur ajoutée et offre des garanties supplémentaires de fiabilité du commerçant.

Ce label de qualité expire après une période déterminée (environ six ou neuf mois). Une nouvelle vérification a lieu peu avant la date d'expiration. La durée de validité du certificat est prolongée pour autant que cette vérification confirme que le commerçant maîtrise encore parfaitement ses transactions électroniques selon les normes établies. Grâce au sceau le consommateur électronique peut effectuer des achats via Internet avec plus de confiance.

Mais ce sceau offre également d'autres avantages :

- un commerçant "virtuel" qui n'a pas obtenu le sceau après un premier audit sait exactement dans quels domaines il doit apporter des améliorations, et peut donc travailler sa qualité de service de manière pro-active. Ceci lui permet également de limiter ses propres risques;

- les autorités disposent d'une garantie minimale quant à la fiabilité des activités commerciales dans le *cyberspace*. Ceci est notamment important dans le secteur financier, où les organes de contrôle prudentiel s'interrogent - et pas tout à fait à tort - sur l'offre virtuelle des sociétés de banque et d'assurances. Le concept pourrait d'ailleurs proposer une solution intéressante à ce sujet, à savoir le développement d'un sceau spécifique qui tiendrait compte des critères spécifiques d'un secteur donné, comme par exemple la loi sur le blanchiment d'argent.

L'institut des Réviseurs d'Entreprises a pris contact avec ses homologues européens dans la perspective de développer un label au niveau européen.

Bruxelles, le 16 décembre 1998.

IV. Les travaux au sein de l'atelier.[32]

1. La labellisation n'est pas une technique de réglementation.

La labellisation de sites *web* consiste à apposer un label de qualité sur un site après qu'il ait été vérifié que le vendeur respecte un certain nombre de critères prédéfinis. Le principal objectif de cette technique est de promouvoir la confiance des consommateurs dans le commerce électronique afin que ceux-ci profitent pleinement du potentiel des nouvelles technologies.

Il ne s'agit donc pas d'une technique de réglementation ni d'un substitut à une réglementation ni d'une réglementation particulière pour le commerce électronique. Son objectif n'est pas de créer un droit du *cyberspace*. La labellisation de sites permet de vérifier a priori si le vendeur respecte certains critères précis.

La labellisation n'empêche nullement les pouvoirs publics d'intervenir d'une manière qu'ils estiment appropriée pour réglementer, le cas échéant, le commerce électronique et ceci ne pose aucun obstacle à l'élaboration et à l'application de codes d'autodiscipline par les organisations professionnelles.

Il est parfois reproché aux codes de bonne conduite élaborés par les professionnels que le consommateur a peu de certitude et de garantie quant au respect de celui-ci par le vendeur. Cette technique de labellisation pourrait également permettre de donner plus de force et d'impact à ces codes d'autodiscipline grâce aux « *assurances* » qui sont apportées aux consommateurs par le tiers certificateur.

Dès lors, la labellisation doit être considérée comme un adjuvant aux différentes réglementations et non pas comme un substitut à une réglementation.

Toutefois, il semble utile de préciser dans ce débat que l'approche développée aux Etats-Unis est différente. Lors de la Conférence interministérielle de l'OCDE tenue à Ottawa du 7 au 9 octobre 1998, Monsieur Ira Magaziner, Conseiller spécial du Président Clinton notamment en matière de commerce électronique, n'a pas caché, lors de son allocution, que, pour lui, la labellisation constituait un moyen efficace pour accroître la confiance des consommateurs dans le commerce électronique et qu'il allait oeuvrer au développement de ce concept. Cependant, il estime que cette technique doit avoir la portée d'un substitut à la réglementation.

L'approche américaine telle que précisée par Monsieur Magaziner s'éloigne donc de l'idée développée au sein de l'atelier.

[32] A plusieurs reprises il est souligné que la labellisation permet d'obtenir une garantie quant à l'identité des acteurs. Il est toutefois important de préciser que lorsque lorsque la Belgique sera dotée d'un cadre juridique relatif aux signatures électroniques, par l'approbation des deux projets de lois, l'identité sera garantie grâce au certficat émis par une A.C. agréée.

2. Une charge supplémentaire pour les vendeurs cybernétiques?

Certains membres de l'atelier expriment leur méfiance à l'égard de labellisation, car ce système ferait reposer sur les vendeurs une charge supplémentaire. Au nom de la non discrimination des formes de commerce, ils pensent qu'on ne peut vérifier a priori si un vendeur respecte certaines législations pour pouvoir exercer une activité commerciale. Dans le monde réel, une personne désirant ouvrir un point de vente ne doit pas, outre les démarches administratives qui incombent à tous (inscription au registre du commerce, inscription à la T.V.A., compte bancaire ou postale, conditions particulières pour certaines professions réglementées,...), démontrer ou justifier préalablement qu'elle respecte certaines législations et règles.

Mais, l'octroi d'un label n'est pas une condition préalable à la vente sur un réseau ouvert. Le vendeur peut solliciter un label à tout moment, avant le lancement de son activité ou après le lancement de celle-ci. Il s'agit d'une démarche volontaire qui n'est nullement obligatoire. Le vendeur soucieux de développer ses ventes sur le *web* profitera de cette opportunité pour informer au mieux les consommateurs et les visiteurs de son site au sujet du respect par lui de certaines règles. En apposant un label sur son site, le vendeur ne fait qu'apporter une information, certifiée par un tiers, notamment sur sa politique commerciale.

Ce système de labellisation n'est qu'une transposition dans le *cyberspace* de principes existants dans le monde réel. Tout un chacun a connaissance de multiples labels figurant sur divers produits et aux significations différentes : un tel label signifie que le contenant du produit est recyclable, un autre signifie que le vendeur verse une contribution financière à un système de collecte et de revalorisation de déchets, un autre affirme que le vendeur respecte certaines normes de sécurité.

Dans le monde réel, un vendeur qui souhaite l'obtention d'un label effectue des démarches librement. Il sait que s'il sollicite un label (exemple : une norme ISO), il doit respecter un certain nombre de critères et il mettra tout en oeuvre pour les respecter. La demande d'un label est une décision des gestionnaires d'une société. Ce principe doit également s'appliquer dans le monde virtuel.

Enfin, la labellisation peut être qualifiée de mouvement en pleine expansion dans le monde réel; le recours à cette technique est de plus en plus fréquent. A titre d'illustration, signalons qu'actuellement un « Label EURO » est projeté. Ce label affiché par le vendeur, certifierait qu'il respecte les règles relatives à l'encadrement de l'Euro.

3. Commerce électronique : un manque de confiance?

L'intitulé de l'atelier indique que les consommateurs hésitent à participer au commerce électronique en raison du manque de confiance qu'ils ont dans l'utilisation

des nouvelles technologies. Nous renvoyons le lecteur à l'introduction dans laquelle différentes justifications sont apportées quant au choix de cet intitulé.

Toutefois, il semble nécessaire de préciser que certains membres de l'atelier pensent que le *cyberspace* est un endroit sûr, et que le manque de confiance n'est qu'un mythe. Le frein au développement du commerce électronique n'est pas le manque de confiance mais bien le coût pour le consommateur (ex: frais de téléphone, frais de transport,). Selon ces personnes, il faut cesser de parler et de débattre autour du manque de confiance. Ces débats ne font que renforcer une idée erronée.

Cette opinion n'est toutefois pas partagée par la majorité des membres qui reconnaissent que si les coûts liés au commerce électronique constituent un frein au développement le manque de confiance est réel et constitue un autre obstacle. D'ailleurs, comme il a été souligné dans l'introduction, les travaux internationaux se préoccupent de ce manque de confiance et s'attachent à la renforcer dans le *cyberspace.*

Lors des débats, il a également été souligné que la confiance créée par le vendeur dans son ou ses points de vente dans le monde réel allait le suivre dans le *cyberspace*. Si cet argument peut paraître pertinent, il faut reconnaître qu'il présente certaines limites. Le commerce électronique est, par essence, de dimension internationale, dès lors les consommateurs ne connaissent pas nécessairement les vendeurs des différents pays. D'autre part, des vendeurs peuvent s'installer sur le réseau sans jamais avoir eu de point de vente dans le monde réel.

4. Information du consommateur.

Etant donné que le but premier de la labellisation est d'augmenter la confiance des consommateurs et de les encourager à recourir au commerce électronique, il est important sous peine d'inefficacité que le consommateur soit informé et sensibilisé à ce système.

Nous avons déjà évoqué, dans ce rapport, l'existence de multiples labels dans le monde réel. Au cours des travaux, certains membres ont attiré l'attention des experts sur une analogie qui peut être faite avec la problématique des labels et étiquetages écologiques (publicité verte) au sujet de laquelle d'aucuns estiment que les consommateurs sont fréquemment « perdus et désorientés » face aux différents labels et étiquetages divers qui viennent se greffer sur les emballages des produits. On est, en effet, en droit de se demander s'ils connaissent la signification de ces labels? Bien souvent, les consommateurs ne connaissent pas la véritable signification d'un label ou ils n'ont qu'une vague idée voire une idée erronée des principes et règlements auxquels ces logos renvoient. Souvent encore, ils confondent la signification d'un marquage réglementaire ou volontaire avec celle d'un autre marquage. Ceci tente à démontrer que les consommateurs sont peu ou mal informés de la portée les labels qu'ils rencontrent au quotidien. Le but du présent atelier n'est pas d'étudier ou de faire le procès des labels existants, mais ce parallèle intéressant et indispensable doit permettre de tirer des le-

çons pour ce qui se passe actuellement afin de garantir, au mieux, la réussite d'une procédure de labellisation de sites Internet.

Une des grandes caractéristiques de l'Internet est de permettre à l'internaute au moyen d'un simple « *clic* » de se rendre directement sur une autre page pour consulter un document auquel il est renvoyé. Il est opportun de profiter de cette fonction d'hyperlien pour informer correctement le consommateur. Ceci pourrait permettre d'éviter ou de limiter les problèmes de sous-information ou de mauvaises informations quant à la signification des labels dont les consommateurs semblent subir les conséquences dans le monde réel.

Il est donc important que le consommateur puisse avoir accès de manière automatique, par un simple clic sur un sigle prédéterminé, aux informations relatives au label. C'est à lui qu'il appartient de prendre l'initiative de consulter ou non ces informations. Celles-ci doivent être claires et compréhensibles. Elles doivent comprendre au minimum des renseignements quant à l'audit et aussi quant à l'auditeur du site concerné. Le consommateur doit pouvoir connaître les critères qui ont servi de base à l'octroi du label, ainsi que le rapport du l'auditeur. Il y a lieu également de prévoir la possibilité pour le consommateur de pouvoir communiquer aisément avec cet auditeur pour lui faire part, le cas échéant, de ses remarques éventuelles. Toutefois, il ne faut pas noyer le consommateur sous un flot d'informations diverses, ce qui pourrait le décourager. Pour ce faire, le rapport complet de l'auditeur devrait, peut-être, être précédé d'un résumé qui permette au consommateur de prendre rapidement connaissance des informations essentielles contenues dans le rapport. En effet, selon l'importance de la transaction, le consommateur ne recherche pas le même niveau de garanties, dès lors il y a lieu de lui éviter la lecture d'une multitude de pages avant d'avoir accès à l'information concrète qu'il recherche.

L'information du consommateur passe également par la sensibilisation et l'éducation par rapport à la procédure de labellisation. Il y a lieu de sensibiliser le consommateur sur la signification des labels. Une sensibilisation et une éducation efficaces devraient être le fruit d'une collaboration et d'une action conjointe des pouvoirs publics, des organisations des consommateurs et des organisations professionnelles.

5. Un label belge?

Le commerce électronique est une illustration de la mondialisation de l'économie, il ne connaît pas de frontière et est donc par essence de type international. On doit toutefois constater qu'actuellement la majorité des sites *web* se trouve aux Etats-Unis et que le nombre des internautes belges ne représente qu'une part infime du nombre des utilisateurs de l'Internet dans le monde. Les relations commerciales sur le réseau entre des vendeurs et consommateurs belges sont minimes. Toutefois, une étude canadienne présentée[33] lors de la Conférence d'Ottawa mettait en évidence que les consommateurs étaient essentiellement tentés d'effectuer des achats nationaux au moyen d'Internet.

[33] Malheureusement nous ne disposons pas, à ce stade, de cette étude ni des chiffres.

Compte tenu de ces éléments on est en droit de se demander si l'élaboration d'un label national est réaliste et utile? Est-il nécessaire de mettre en place un tel projet compte tenu de cette dimension internationale?

Les membres de l'atelier sont tous conscients qu'une initiative se limitant au seul niveau belge a peu de signification et qu'il est nécessaire d'avoir, au minimum, un système de labellisation au niveau européen. Mais cela ne signifie pas pour autant que nous devons adopter une attitude attentiste et purement passive.

La poursuite de la réflexion au niveau belge permet de faire mûrir l'idée et de porter sur la scène européenne un projet et/ou des principes concrets. Les initiateurs du projet belge sont également conscients de la nécessité de donner une dimension internationale à leur projet et, à cet égard, ils ont d'ailleurs entrepris différents contacts avec des homologues de différents pays et avec la Commission Européenne afin de faire progresser l'idée.

Une des grandes problématiques liée au développement du commerce électronique est la question du droit applicable. Ce débat est loin d'être clos. Les travaux du présent atelier n'avaient pas pour objet l'étude de cette question, mais il semble utile d'apporter certaines précisions dans le cadre de ce rapport.

Une incertitude relative existe quant aux règles qui doivent s'appliquer à la transaction commerciale entre un vendeur d'un pays déterminé et un consommateur d'un autre pays. Cette incertitude et ce débat sont renforcés par la multitude de législations et de règles différentes existantes au niveau mondial. L'harmonisation des règles au niveau international ne saurait que réduire considérablement ces incertitudes. Dès lors, il semble opportun que l'OCDE poursuive ses travaux relatifs à l'élaboration de lignes directrices relatives à la protection des consommateurs dans le cadre du commerce électronique. Lors de la Conférence d'Ottawa, les ministres ont insisté sur la nécessaire poursuite des travaux et ont souhaité leur aboutissement courant 1999. Sur le plan européen, un effort d'harmonisation constant est entrepris pour lever les entraves au marché intérieur. L'adoption de la directive relative aux contrats négociés à distance devrait avoir pour conséquence à moyen terme une harmonisation minimale des règles dans les quinze états membres, reposant sur des mêmes principes en la matière.

Dès lors, il semble nécessaire que la labellisation de sites porte sur des critères et des normes définis sur le plan international. Un premier effort devrait tout d'abord porter sur la création de labels portant sur le respect des normes européennes.

D'autre part, il ne faut pas perdre de vue qu'outre-Atlantique la labellisation est déjà effective. Les sociétés qui ont développé les labels américains aspirent à exporter leur concept sur le continent européen. Toutefois, nous avons déjà signalé qu'il existait une différence dans l'approche que le gouvernement américain pourrait avoir sur la portée de la labellisation. Si les Etats-Unis désirent faire du principe de labellisation de sites un de leurs atouts pour développer le commerce électronique, il est logique de penser qu'ils tenteront d'imposer leur philosophie en Europe. D'ailleurs, *Webtrust* a

déjà pris des contacts en Europe et accorder des licences à des sociétés pour réaliser des audits, en vue de la délivrance de son logo à des sites européens.

Dès lors, si nous restons passifs en Belgique et en Europe, les sociétés américaines vont labelliser des vendeurs belges et européens selon des critères ayant cours aux Etats-Unis. Une fois cette percée significative réussie sur notre marché, il sera difficile pour les sociétés belges et européennes d'entrer dans la partie et de prendre part au système. Par ailleurs, les critères de labellisation « à l'européenne » seront, certainement, différents tant en matière de vie privée que de fiscalité ou de protection des consommateurs des critères américains.

De plus, n'oublions pas qu'une des incertitudes liées au développement du commerce électronique est son impact sur le volume d'emplois. Les études diverses sont contradictoires. Lors de la Conférence d'Ottawa, les Ministres ont demandé à l'OCDE de poursuivre ses travaux relatifs à l'impact socio-économique du développement du commerce électronique. La labellisation des sites est un moyen de créer, dans un premier temps, des emplois liés à la société de l'information et d'autre part, si elle arrive à démontrer son efficacité dans les faits, elle pourrait avoir un effet de boule de neige en augmentant l'offre et la demande sur les réseaux.

En conséquence, il y a lieu, d'une part, de poursuivre la réflexion en Belgique et, d'autre part, de mettre tout en oeuvre pour que les travaux aient rapidement lieu sur la scène européenne, afin d'établir une plate-forme commune entre les Etats membres.

Le principe de la reconnaissance mutuelle devrait permettre aux sociétés belges de labelliser des sites étrangers et aux vendeurs étrangers de pouvoir être labellisés en Belgique.

Plus le projet sera mûri en Belgique, plus la Belgique jouera un rôle majeur sur la scène internationale

6. Un label ou plusieurs labels.

Il est incontestable que le concept de labellisation de sites Internet va conduire à l'apparition de multiples labels soit en fonction des acteurs qui interviennent dans sa délivrance soit en fonction de l'objet de la labellisation. Ainsi, à priori on peut penser il y aura des labels qui certifient des aspects particuliers, à l'instar de *Trust-E* aux Etats-Unis. Ainsi, le label « A » va certifier que le vendeur respecte les règles relatives à la protection de la vie privée, un label « B » se contentera de certifier l'identité du vendeur, un label « C » donnera des garanties quant à la sécurité du site du vendeur, un autre label certifiera que le vendeur respecte les règles relatives à la protection des consommateurs, une autre label pourrait être fonction des lois fiscales.... D'autre part, il y aura un label qui correspond à une certification globale qui porte sur différents éléments (cfr. le projet belge *de l'IRE)*Enfin, il peut se produire l'apparition de labels spécifiques par secteur, par exemple, un label spécifique pour les produits financiers.

Ces approches présentent à la fois des inconvénients et des avantages qu'ils semblent utiles d'énoncer ici.

Une labellisation multiple sur des aspects particuliers risque de conduire à une prolifération de labels. Une page *web* d'un vendeur pourrait se voir garnie d'une multitude de labels correspondant chacun à un certificat différent portant sur des aspects particuliers. Ceci pourrait conduire à réduire, voire encore à anéantir les effets recherchés en semant le trouble chez les consommateurs.

Une labellisation par secteur permet de prendre mieux en considération les spécificités propres de certains secteurs. Un audit d'un site proposant la vente de service financier ne peut se faire sur base des mêmes critères qui sont utilisés dans le cadre d'un audit portant sur un vendeur de livres en ligne.

Une multi-labellisation permettrait un contrôle plus spécifique. Ceci offre l'avantage que l'audit particulier qui sera réalisé sera plus précis.

Une labellisation globale offre l'avantage pour le consommateur d'avoir un aperçu général de la politique commerciale menée par le vendeur et de l'organisation de ce dernier. Mais cette procédure est forcément plus onéreuse que la première, étant donné que l'audit servant de base portera sur un nombre plus important de points.

Les membres de l'atelier ne préfèrent pas un système à un autre, mais ils s'accordent pour affirmer que la labellisation doit se faire dans le respect des règles du droit de la concurrence.

C'est au vendeur qu'il appartient de déterminer, en fonction des produits et/ou services qu'il vend, le type de label qui, selon lui, pourrait le mieux répondre aux attentes des consommateurs et/ou acheteurs potentiels. En effet, selon le type de produits ou de services offerts en vente, les attentes de ces derniers seront différentes.

7. Sécurité du label.

Un membre a tenu à attirer l'attention de l'atelier sur le fait que le label « *Trust-E* » pouvait être copié facilement. Ceci peut évidemment conduire à des malversations ou abus qui risquent de discréditer le principe de labellisation.

Le label qui se présente sous la forme d'un sceau qui apparaît à l'écran du site du vendeur doit être sûr. Il y a lieu de veiller à ce que le label soit entouré d'un maximum de garantie de sécurité afin qu'il ne puisse être copié ou falsifié. La sécurité du label doit être non seulement technique mais aussi juridique. Le logo du label doit être protégé juridiquement de façon adéquate afin d'éviter toute utilisation non appropriée par des tiers.

Pour éviter tout abus, la possibilité du retrait d'un label ne peut qu'appartenir à l'organe qui l'a octroyé et apposé sur le site.

8. Coût du label.

La certification d'un site présente inévitablement un coût. Aucun chiffre précis n'a été avancé dans le cadre des travaux de l'atelier. Le coût sera inévitablement variable et fonction du travail demandé pour réaliser l'audit. L'audit relatif à un site qui offre en vente des services financier sera inévitablement plus cher que celui qui examinera les pratiques du sites vendant des livres ne ligne.

Le coût du label ne se limite pas à son octroi. Le label est octroyé pour une période déterminée; à l'issue de celle-ci un nouveau contrôle et des vérifications sont effectuées pour déterminer si le vendeur répond toujours aux critères d'octroi. Ces procédures récurrentes ont également un coût.

Les membres de l'atelier estiment toutefois que le coût ne peut être prohibitif, afin de ne pas exclure les P.M.E. de la possibilité de solliciter un label.

9. Critères servant de base à l'octroi d'un label.

Au cours de ce rapport, nous avons précisé que l'octroi du label se faisait à la suite d'un audit qui veille à établir que le vendeur respecte des critères préétablis. L'atelier s'est penché sur ces critères et a essayé de déterminer s'il y avait lieu de les préciser.

Ces critères seront évidemment variables. Ils seront, bien évidemment, différents selon que l'on se situe dans le cadre d'une labellisation globale ou qui porte seulement sur un point particulier. Il semble impossible et inopportun de définir de manière exhaustive et limitative ces critères. En effet, les attentes des consommateurs sont différentes selon qu'ils souhaitent acheter un compact-disc, une assurance ou réserver un voyage.

D'ailleurs, les initiateurs du projet belge ont tenu à préciser qu'ils ont mis au point un guide pratique destiné à l'auditeur. Il ne s'agit pas d'une liste de questions limitatives et impératives auxquelles l'auditeur est tenu de répondre de façon complète. Cette liste est un outil devant aider à l'analyse et, l'auditeur reste libre d'exercer sa mission en tenant compte des spécificités propres au cas d'espèce dont il procède à l'analyse. Ils estiment qu'il faut laisser une place au jugement de l'expert et du professionnel.

Les membres s'accordent à dire qu'il ne revient pas aux pouvoirs publics de définir précisément l'intégralité de ces critères[34]. Ils pourraient toutefois être associés à l'élaboration de ces principes, les associations de consommateurs et professionnels pourraient également être conviées à participer à ces travaux.

Il ne semble pas inutile de préciser que la labellisation de sites ne visent nullement à certifier la qualité des produits et services vendus et qu'en conséquence les critères ne portent pas sur cet aspect particulier.

[34] Voir également infra 12, le rôle des pouvoirs publics en matière d'homologation.

Enfin, il est nécessaire que l'octroi du label soit limité dans le temps et qu'il soit procédé régulièrement à un nouvel examen des critères afin de s'assurer de manière continuelle du respect de ceux-ci par le vendeur. En cas de plainte d'un consommateur, l'auditeur devrait vérifier si celle-ci est fondée et intervenir de manière appropriée, le cas échéant, auprès du vendeur. Des procédures de révocation ou de suspension du label devraient être envisagées.

10. Responsabilité.

L'octroi d'un label doit faire reposer sur l'entité qui l'a délivré une responsabilité à l'égard des tiers. Toute absence de responsabilité ou une responsabilité limitée risquerait de réduire à néant la valeur d'un label.

L'entité qui délivre un label doit être responsable. Sa responsabilité ne peut se limiter à l'octroi du label. L'organe certificateur doit mettre en place des procédures de contrôle efficaces et effectives (*hot-line*, contrôles d'initiative). Les contrôles de l'organe certificateur seront également fonction du secteur concerné. Au plus la valeur des transactions ou les conséquences de celles-ci sont élevées au plus les procédures de contrôles devraient être importantes.

11. Une autolabellisation.

Lors des travaux, un membre a émis l'idée d'une autolabellisation. Sous ce vocable, on peut distinguer deux systèmes différents.

D'une part, dans le cadre d'un label général qui fixe les principes à respecter, le vendeur déclarerait au moyen d'assertions sa politique commerciale et son respect des principes.. Il envoie cette déclaration à l'entité qui délivre un label sur base de cette déclaration d'engagement. Dans cette hypothèse, il n'y a pas d'audit externe à priori.. Par ce système, le vendeur se rendrait directement responsable auprès du consommateur de ses engagements.

Ce système est moins onéreux en raison de l'absence d'audit externe à priori. L'audit externe n'intervient que lors de contrôles ponctuels ou à la demande ou sur plainte d'internautes.

D'autre part, le vendeur pourrait uniquement indiquer sur son site sa politique commerciale (« company policy ») sans aucune référence à un quelconque label comme général, et déclarer qu'il s'engage à la respecter. Ceci pourrait s'assimiler à une publicité et dès lors entraîner une certaine responsabilité. Dans cette hypothèse le vendeur pourrait-il s'attribuer un label de qualité qu'il s'auto-attribuerait?

Le débat sur ce point a clairement mis en évidence qu'il était nécessaire de procéder à une analyse en profondeur sur la responsabilité des différents intervenants.

12. Les différents acteurs dans la labellisation.

Dans le principe de la labellisation, on peut distinguer deux fonctions essentielles. D'une part, il y a la fonction d'audit, qui consiste à vérifier si le vendeur respecte les critères prédéfinis et, d'autre part, il y a la gestion du label qui doit être entouré de certaines garanties.

Plusieurs questions peuvent être mises en évidence, par exemple est-ce que ces deux fonctions doivent ou peuvent être remplies par une même société? Les questions de responsabilités doivent être également analysées au regard de ces fonctions différentes.

Il est nécessaire de veiller à ce que les personnes qui pratiquent les audits soient indépendantes des vendeurs, une procédure d'agrément pourrait être envisagée

13. Rôle des pouvoirs publics dans le système de labellisation

Les pouvoirs publics doivent-ils être parties prenantes dans la labellisation de sites et dans quelle mesure? Doivent-ils favoriser la labellisation? Quel doit être leur rôle? Voici un bref échantillon des questions qui ont été avancées pendant les travaux. Cette question du rôle de l'Etat est transparue en filigrane tout au long des travaux. C'est volontairement que nous tentons de synthétiser les avis émis sur cette question en fin de rapport car elle renvoie souvent aux points développés ci-avant.

Un membre estime que les pouvoirs publics n'ont pas à se préoccuper de la labellisation des sites, une action des pouvoirs publics ne saurait que ralentir les choses et d'empêcher les nouvelles initiatives. Toutefois, il s'agit d'un avis minoritaire.

D'une manière générale, les membres de l'atelier estiment que les pouvoirs publics ne doivent pas avoir un rôle premier dans ce système. L'initiative et la gestion de la labellisation doivent appartenir au secteur privé. L'affirmation d'un tel principe ne signifie pas pour autant un retrait total des pouvoirs publics en la matière. Au contraire, une action est même souhaitée dans certains domaines.

Nous avons déjà signalé, ci-avant, qu'il n'appartenait pas à l'Etat de définir les critères servant de base à l'attribution de labels. En effet, on ne peut exiger qu'une audit porte sur toutes les législations en vigueur. Dès lors, si l'on demande aux pouvoirs publics de déterminer les critères, ils devraient opérer une sélection entre les différentes législations et créer ainsi une sorte de hiérarchie entre les différentes réglementations. Ceci ne semble pas réaliste. Toutefois, on pourrait imaginer que les pouvoirs publics fixent certains critères obligatoires, par exemple : la localisation géographique du vendeur.

Tout comme il n'appartient pas aux pouvoirs publics de définir les critères, il n'appartient pas à l'Etat de délivrer personnellement les labels. Un label constitue une

publicité au sens de l'article 22 de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur qui dispose :

> *« Pour l'application de la présente loi, est considérée comme publicité, toute communication ayant pour but direct ou indirect de promouvoir la vente de produits ou services, y compris les biens immeubles, les droits et les obligations, quel que soit le lieu ou les moyens de communication mis en oeuvre ».*

S'il appert qu'un vendeur appose un label et qu'en fait, il s'agit d'une publicité trompeuse alors que l'Etat a octroyé un label, il pourrait être considéré comme ayant cautionné une publicité trompeuse.

Si les membres reconnaissent que le rôle de l'Etat en la matière doit être secondaire, ils s'accordent à dire que les pouvoirs publics ont, par contre, un rôle important à jouer favorisant le développement et la diffusion des labels et en promouvant des labels de bonne qualité.

Ainsi, les membres de l'atelier ont pris connaissance avec intérêt du projet de modification de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur adopté par le Conseil des Ministres le 24 juillet 1998, et plus particulièrement son article 80§3 dernier alinéa qui prévoit :

> *« L'interdiction visée au premier alinéa[35] est levée lorsque le vendeur apporte la preuve qu'il respecte les règles fixées par le Roi en vue de permettre le remboursement des sommes versées par le consommateur ».*

L'exposé des motifs de ce projet est clair sur la volonté poursuivie par cette disposition :

Cet « *article prévoit que l'interdiction d'exiger des paiements préalables du consommateur avant la fin du délai de renonciation pourra être levée pour les vendeurs qui présenteront des garanties de remboursement dans le cadre d'un système répondant à des critères fixés par le Roi. Un système de cautionnement, de blocage transitoire des sommes versées, d'assurance ou de labellisation assurant un gage de qualité - notamment des sites de commerce électronique - pourrait ainsi être défini par le Roi. Le but est de garantir au consommateur un remboursement facile et rapide des sommes versées* ».

Ce projet crée une première ouverture pour une reconnaissance officielle de la labellisation de *sites-web* et la majorité des membres approuvent cette initiative. Certains membres souhaitent toutefois attirer l'attention sur le fait qu'en la matière, s'il y a lieu de prévoir des procédures dérogeant à l'interdiction aux pré-paiements dans le commerce hors ligne, il est nécessaire de prévoir également un tel système dans le monde réel, c'est-à-dire pour la vente à distance que nous pouvons qualifier de classique ou traditionnelle.

[35] Il s'agit, dans le cadre de vente à distance, de l'interdiction pour le vendeur d'exiger un acompte ou un paiement avant la fin du délai de renonciation.

L'absence de tout cadre juridique en matière de labellisation risquerait de voir l'apparition de labels « farfelus » qui risqueraient de discréditer le principe; il y a lieu de veiller notamment à ce que les organes qui attribuent les labels soient complètement indépendants. Ce cadre juridique doit être minimal et neutre d'un point de vue technologique afin de ne pas étouffer l'innovation.

Par ailleurs, l'Etat aura à coeur d'éduquer l'internaute à l'intérêt et à la signification des labels. Il faut également prévoir dans l'activité d'organes existants, ainsi services administratifs du Ministère des Affaires économiques, le Conseil de la Consommation ou la Commission de Protection de la Vie Privée des mécanismes souples d'homologation des labels.

Signalons aussi qu'afin de favoriser le développement de la certification des *sites web* et l'apparition d'entraves nationales au sein de l'Union Européenne, un cadre juridique légal européen n'est pas à exclure et même souhaité.

Enfin, l'attention du lecteur est portée sur les recommandations figurant in fine de ce rapport où le rôle des pouvoirs publics apparaît clairement dans le cadre juridique à mettre en place.

V.RECOMMANDATIONS

PRINCIPES

L'Atelier insiste sur la nécessité de donner une dimension européenne au projet de labellisation de sites et demande à Monsieur Di Rupo, Vice-Premier Ministre, de prendre toutes les initiatives nécessaires à cette fin.

L'Atelier prône le respect des principes suivants :

1. NON AUTOSUFFISANCE : La labellisation ne peut être un substitut à la réglementation ; elle représente un moyen supplémentaire d'apporter des garanties quant au respect de la réglementation légale ou d'autodiscipline ou d'engagements propres au vendeur et permet aux utilisateurs des sites *Web* ou à l'Etat d'être assurés à priori d'un tel respect.

2. CARACTERE VOLONTAIRE : La labellisation doit avoir un caractère non obligatoire. Les sites *Web* ne peuvent en aucune manière être contraints d'adopter un label.

3. PRIX ABORDABLE : L'octroi de labels ne peut s'opérer à des prix dissuasifs, ce qui ne permettrait pas à des PME de les obtenir.

4. DANS UN MARCHE CONCURRENTIEL : Il est exclu que d'une manière ou d'une autre soit consacré un monopole quant à la délivrance des labels.

Le marché doit être libre et concurrentiel. Sans doute, regretterait-on une trop grande profusion de labels qui conduirait à la confusion des consommateurs. Il faut que le consommateur puisse se fier à tous les labels décernés sous peine d'un échec de l'objectif recherché par le principe de la labellisation.

5... TRANSPARENT : Il importe que l'autorité en charge de la délivrance, la procédure suivie et les critères appliqués lors de l'examen de la délivrance du label soient transparents et puissent facilement être accessibles à l'internaute (via hyperlink, par exemple).

6... ET RESPONSABLE : L'octroi d'un label doit entraîner pour celui qui le délivre une certaine responsabilité à défaut de quoi sa valeur risque d'être réduite. Il est nécessaire que celui qui délivre le label ait souscrit une assurance qui couvre sa responsabilité professionnelle et qu'il soit soumis au secret professionnel ou à une obligation équivalente.

ROLE DE L'ETAT

1. LE SECTEUR PRIVE PREMIER RESPONSABLE : Il n'appartient pas à l'Etat de définir lui-même les critères de labellisation. Le secteur privé est le premier responsable de leur définition. Ceci n'exclut pas des concertations avec les pouvoirs publics et les associations de consommateurs.

2. ROLE SUBSIDIAIRE DE L'ETAT : L'affirmation des principes affirmés ci-dessus est par contre du ressort de l'Etat.

3. ENREGISTREMENT DES LABELS : L'Etat peut en outre, selon la procédure comparable à celle de l'enregistrement des codes de conduite en matière de vie privée, procédure prévue par l'article 28 de la directive de protection des données, soumettre les projets de label élaborés en toute indépendance, au contrôle de leur conformité à la réglementation. Cet enregistrement pourrait s'opérer avec le concours d'autorités existantes (Autorités de contrôle de la Vie Privée ; Conseil de la Consommation) ou d'administrations concernées.

4. ENCOURAGEMENT ET EDUCATION : L'Etat se doit d'encourager la labellisation par des références légales ou par l'octroi d'avantages légaux aux labels, le cas échéant, enregistrés (cf. à cet égard, l'avant-projet de loi de protection des consommateurs, art. 80 § 3 qui apparaît comme une bonne mesure).

Une campagne de sensibilisation des internautes à l'existence, à la valeur des labels doit être organisée.

CRITERES DE QUALITE DES LABELS

Outre le caractère de transparence sur la qualité de l'auteur du label, la procédure suivie et les critères d'attribution du label, il importe que

1. le label soit sûr : c'est-à-dire qu'il ne puisse faire l'objet de copiage et que son attribution ou son retrait ne puissent faire l'objet de manipulations discrétionnaires par celui qui reçoit le label ou par une tierce partie

2. le label doit être contrôlé et/ou attribué par une autorité offrant des garanties d'indépendance et d'impartialité.

3. le respect du contrôle des conditions d'octroi du label et les sanctions en cas de non respect des engagements doivent être EFFECTIFS à travers des mécanismes divers : audit par des sociétés tierces, mise sur pied de *hot-lines*, période limitée d'attribution des labels, procédure de révision,...

PROLONGATIONS SUGGEREES

L'atelier est conscient que les débats n'ont pas permis de répondre à toutes les questions et estime nécessaire que la réflexion soit approfondie sur certains points, et plus particulièrement :

1. la responsabilité des organes de labellisation et des sociétés utilisant les labels;

2. le rôle de l'Etat, en particulier les mesures et initiatives qui devraient être prises par le Ministère des Affaires économiques.

3. la protection légale et technique des labels.

Bruxelles, le 16 décembre 1998.

TABLE DES MATIERE DES ANNEXES

Bruxelles, le 16 décembre 1998.